IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff	)	
	)	
-VS-	)	Criminal No. 21-10104-PBS
	)	Pages 7-1 - 7-167
VLADISLAV KLYUSHIN,	)	
	)	
Defendant	)	

JURY TRIAL - DAY SEVEN

BEFORE THE HONORABLE PATTI B. SARIS
UNITED STATES DISTRICT JUDGE

United States District Court
1 Courthouse Way, Courtroom 19
Boston, Massachusetts 02210
February 7, 2023, 9:10 a.m.

LEE A. MARZILLI
OFFICIAL COURT REPORTER
United States District Court
1 Courthouse Way, Room 7200
Boston, MA 02210
leemarz@aol.com

A P P E A R A N C E S:

SETH B. KOSTO, ESQ. and STEPHEN E. FRANK, ESQ., Assistant United States Attorneys, Office of the United States Attorney, 1 Courthouse Way, Room 9200, Boston, Massachusetts, 02210, for the Plaintiff.

MAKSIM NEMTSEV, ESQ., 20 Park Plaza, Suite 1000, Boston, Massachusetts, 02116, for the Defendant.

MARC FERNICH, ESQ., Law Office of Marc Fernich, 800 Third Avenue, Suite Floor 20, New York, New York, 10022, for the Defendant.

I N D E X

P R O C E E D I N G S

THE COURT: The jury is all ready here. Is your agent here?

MR. FRANK: Yes.

THE CLERK: You can take the stand, and then the interpreters are still under oath?

THE COURT: Yes.

You're up at bat, right?

MR. FRANK: Yes, I am.

09:11 THE COURT: Knock on the door, Maryellen.

THE CLERK: I have to make sure his headphones are -- working. Max, put him on 28 on the back side of it.

(Discussion off the record.)

THE COURT: By the way, Maryellen got a phone call that a sketch artist may be coming. I don't know if anyone is familiar with that. So a sketch artist may be arriving tomorrow or the next day or whatever.

MR. FERNICH: I'm glad I wore this fancy shirt and tie today.

09:12 THE COURT: Yes, but you've got to turn and face her for them to see the purple --

(Laughter.)

MR. FERNICH: I'll handle that part of it.

THE COURT: Very, very, very stylish. So, all right, let's let this jury in.

THE CLERK: All rise for the jury.

(Jury enters the courtroom.)

THE COURT: Good morning to everyone.

THE JURY: Good morning.

THE COURT: Once again, you're the most amazing jury ever. You're all showing up on time, and I know the weather is cold, et cetera, and so -- not as bad as it was on Friday, but nonetheless.

Someone asked me about the trial and what to expect in
09:12 terms of timing. We're right on track, let me start there; if anything, a little on the earlier side. So there's no way it's going to go beyond, you know, the long weekend. I'm hoping actually that it could possibly finish, in terms of the evidence, end of week, beginning of next. On the day or days you're out deliberating and closings, et cetera, I'll ask you probably to stay till 4:00 o'clock, so please sort of be flexible towards the end of the week, beginning of next as to when that is.

How long the trial takes is ultimately up to you for
09:13 as long as it takes to deliberate. So somebody asked for that. I think someone had a doctor's appointment. And unfortunately Monday is, like, right on -- I don't know what Monday is going to look like.

Anyway, I think that's all we need. Did anyone talk about the case, see anything in the newspaper, social media?

Anyone try to get in touch with you? I find the jury has complied.

Let's move on. We're going to finish on the recross?

MR. NEMTSEV: Recross.

THE COURT: Okay, and then on to the next witness.

THE CLERK: Sir, you're still under oath.

THE WITNESS: Yes, ma'am.

THE CLERK: Thank you.

DAVID HITCHCOCK

09:14 having been previously duly sworn, was examined and testified further as follows:

THE COURT: You have notebooks? Everyone ready?

MR. NEMTSEV: May I proceed, your Honor?

THE COURT: Absolutely. Go ahead.

CONTINUED RECROSS-EXAMINATION BY MR. NEMTSEV:

Q. Good morning, Special Agent Hitchcock.

A. Good morning.

Q. You testified on redirect that StackPath's document retention policy is three years, correct?

09:14 A. In certain aspects, it was represented that way, yes.

Q. And so did the government and FBI agents obtain invoices from Micfo directly?

A. Could you repeat the question, please.

Q. Did you obtain any invoices directly from Micfo that came from other government agents?

A. Yes.
Q. And you would agree that those government agents obtained them as part of Micfo's criminal case?
MR. FRANK: Objection, your Honor.
THE COURT: Overruled.
A. Yes.
Q. And you would agree that they obtained those invoices close in time to the indictment of Micfo?
A. I don't know.
09:15 Q. You would agree that they obtained them prior or at the time of Micfo's indictment, correct?
A. That's my understanding.
Q. And Micfo was indicted in the spring of 2019, correct?
A. I don't know the timing, sir.
Q. Micfo was indicted after December of 2018, correct?
A. I believe that's correct.
Q. And if I represent to you that Micfo was indicted in the spring of 2019 --
MR. FRANK: Objection.
09:15 THE COURT: Sustained. He said he didn't know.
Q. And isn't it a fact, sir, that you did not look at any additional invoices relating to the 104.238 IP address from the production that Micfo sent directly?
A. I believe that's correct, yes.
Q. You testified on redirect that the Wan Connie account used

the inbox.lv address; is that correct?
A. Yes.
THE COURT: Wait a minute. Slow down again so we remember. What's the Wan Connie account?
THE WITNESS: This was one of the accounts obtained in the course of the investigation. It was a Namecheap account.
Q. And isn't it a fact, sir, that the Wan Connie email address doesn't fit the labeling that you described on the other Namecheap accounts related to the intrusions or potential
09:16 intrusions into Toppan Merrill servers?
A. It was very similar. It was first, last, and three letters instead of two at inbox.lv.
Q. But it was not the same, correct, sir?
A. It was very similar, yes.
THE COURT: Slow down because we don't know this as -- so say it again. It was the first --
THE WITNESS: Oh, first as in first name, last as in last name of the subscriber, three letters instead of two at inbox.lv. And by three -- I think I said three letters. I
09:17 meant three numbers, so wanconnie90@inbox.lv.
Q. And, to your knowledge, anyone can create an account within the inbox.lv; is that correct?
A. That's my understanding. It's just open to the general public.
Q. And isn't it a fact, sir, that the Wan Connie account did

not purchase any of the domains that were located on Toppan Merrill servers?
A. That's correct.
Q. And, sir, do you deny that Special Agent Kang reviewed the M-13 website prior to Mr. Klyushin's arrest?
MR. FRANK: Objection as to what Special Agent Kang did.
THE COURT: Sustained.
MR. NEMTSEV: Nothing further, your Honor.
09:18 THE COURT: Okay, thank you. You may step down.
THE WITNESS: Thank you.
(Witness excused.)
MR. FRANK: The government calls Jacob Wall.

JACOB WALL

having been first duly sworn, was examined and testified as follows:
THE CLERK: You can be seated. Could you please state and spell your last name for the record.
THE WITNESS: Wall, W-a-l-l.
09:19 DIRECT EXAMINATION BY MR. FRANK:
Q. Good morning, Mr. Wall. Could you just pull that mic up close. Are you currently employed?
A. Yes, I am.
THE COURT: No. We can't hear a word you're saying.
THE WITNESS: Yes, I am.

THE COURT: All right, let's practice. What's your full name?

THE WITNESS: Jacob Wall.

THE COURT: All right, you hear your voice catch? So we all need to hear you. Okay, great. Thank you.

Q. Where do you work, Mr. Wall?

A. I'm a pilot for a private charter company out in El Paso called ATI Jet.

Q. And is that what you were doing in 2018?

09:19 A. No. I worked for StackPath back then.

Q. Can you just speak a little louder and a little more slowly, please.

A. I worked at StackPath back then.

Q. What was StackPath?

A. StackPath was a business that had a business-to-business component as well as business-to-consumers side, and I worked on the business-to-consumers side VPN services.

Q. It provided VPN services?

A. Yes.

09:20 Q. Did StackPath have any subsidiary or related companies?

A. Yes. They had quite a few.

Q. Could you tell me what some of those were.

A. IPVanish, StrongVPN, and Encrypt.me.

THE COURT: You know what, we have to get them down. So we have -- all right, so slow down. All right, we don't

know these names. Some of them we've heard; some of them we haven't. So slow down. So what did StackPath have? Was it affiliated businesses? Was that the way you -- how did you word it? Why don't you --

MR. FRANK: Subsidiary or related businesses.

A. So some of the subsidiaries were IPVanish, StrongVPN, and Encrypt.Me.

THE COURT: What was that last one?

THE WITNESS: Encrypt period me, so Encrypt.me.

09:20 Q. And was there also an affiliated business called Mudhook Marketing?

A. Yes. Mudhook Marketing was the legal entity that owns IPVanish.

Q. And those other entities were VPN providers?

A. Yes.

Q. How long did you work at StackPath?

A. I started in July of 2016, and Ziff Davis acquired them in April of 2019.

Q. Ziff Davis acquired them in April of 2019?

09:21 A. Yes.

Q. And Ziff Davis is a large publicly traded company?

A. Yes.

Q. What were you doing for StackPath in 2018?

A. I was the director of business operations, so I focused on global expansion, understanding how we could better improve the

service for our customers, and had my hands in a lot of different areas there.

Q. How far did you go in school, sir?

A. I got my bachelor's degree.

Q. In what?

A. General business from SMU.

Q. Directing your attention to late 2017, early 2018, did there come a time when StackPath decided to enter the Boston Market?

09:22 A. Yes.

Q. Why did you want to be in Boston?

A. So 2017 was the year where there was a ton of growth within that business, so I had made a goal to be within 250 miles of any of our users and customers in the United States, so we expanded to multiple cities. The idea behind it is that the service is better the closer you are to the end user.

Q. Why is the Internet service better the closer you are to the end user?

A. So there is latency, so if you're trying to connect to the

09:22 Internet and you have to go from, say, Boston to Dallas to go back to Boston, that roundtrip time makes a not as good user experience.

Q. So you wanted to be in Boston to provide better, faster Internet service to your clients?

A. Yes.

Q. As part of that effort, did there come a time when you leased a set of IP addresses from a company called Web2Objects?
A. Yes.
Q. What is Web2Objects?
A. They owned a lot of IP addresses that we leased from them in a variety of states in the U.S. and countries abroad.
Q. Why did you lease the addresses from Web2Objects as opposed of buying them?
A. So the idea behind leasing was that it would save us money in the short term because they were quite expensive to purchase outright.
Q. Were IP addresses limited at that time?
A. Yes. At that point, all of the IP addresses had been allocated, so you had to purchase them on the secondary market.
Q. And so you leased them from Web2Objects?
A. Yes.
MR. FRANK: Could we have Exhibit 145 in evidence, please.
Q. Mr. Wall, do you see this letter of authorization from Web2Objects to a company called Micfo?
A. Yes.
Q. What is a letter of authorization?
A. A letter of authorization is a form that the owner of the IP addresses makes which allows us to announce them, to make them accessible on the Internet.

Q. Announcing an Internet address makes it accessible on the Internet?

A. Yes.

Q. What is Micfo?

A. Micfo was a provider that we used to get servers in Internet transit from -- out to multiple cities in the U.S.

THE COURT: Slow down. What is it?

THE WITNESS: A company that we rented servers from.

Q. And you said you rented servers from Micfo in multiple cities in the United States?

09:24

A. Yes.

Q. And at this time, May 2018, had you been using Micfo for those types of services?

A. Yes, we had.

Q. Okay. And what was your experience with Micfo?

A. Very good. They had a bunch of locations that were harder for us to acquire. They were unique, in that they picked cities that there wasn't a lot of competition in in order to, you know, be the player out there.

09:24

THE REPORTER: Please repeat the last part.

THE WITNESS: Oh. In order to be competitive in that area.

THE COURT: You drop the end of your sentences, which is why we're not catching the end.

THE WITNESS: Okay. Can you restate that question,

and then I'll --

Q. I'll move on to the next question. Thank you. In this letter we see references to a 104.238.37.0/24 block of IP addresses?

A. Yes.

Q. And so am I correct in understanding that there are numerous individual IP addresses within that block?

A. Correct, and the slash 24 was 255 IPs.

Q. And they all began with 104.238.37?

09:25 A. Yes.

Q. Okay. And those were assigned to Boston?

A. Yes.

Q. And then you have other IP addresses, 104.238.38 for Cleveland, 45.56.172 for Denver, and so on and so on in cities including Milwaukee, Nashville, Salt Lake, and St. Louis?

A. Yes.

Q. And you used Micfo to provide those services to you?

A. Correct.

Q. Now, this letter of authorization -- by the way, did you

09:26 receive this letter of authorization?

A. Yes.

Q. And the letter is dated May 30th of 2018. Do you see that?

A. I do.

Q. What was your practice when you received a letter of

authorization like this?
A. We would immediately provide it -- or I would immediately provide it to, in this case, Micfo.
Q. I want to ask you a question about a company called Cogent. What is Cogent?
A. Cogent is what is called a tier one network, so they have access to everyone on the Internet. So they're a company not many people know but is the backbone to the Internet.
Q. It's the backbone to the Internet?
09:27 A. One of three, yes.
Q. So it's like a pipeline for Internet traffic?
A. Yes.
Q. Okay. And when you rented servers from Micfo in Boston, do you have an understanding of who the Internet service backbone provider was for the Boston datacenter?
A. Yes, Cogent.
Q. Given this letter of authorization, was Cogent authorized to direct Internet traffic for the 104.238.37 block of IP addresses anywhere other than Boston?
09:27 A. No. Just Boston.
Q. You testified that you provided this letter of authorization to Micfo right away.
A. Yes.
Q. Why?
A. It was standard practice. There's a lot of cost involved

in renting these IP addresses and the associated servers, so it was in our best interest to get things up and running as quickly as possible.

Q. As of May 30, 2018?

A. Yes.

MR. FRANK: Could we have Exhibit 140, please.

Q. Mr. Wall, this is Exhibit 140 in evidence. Do you recognize it?

A. Yes.

09:28 Q. What is it?

A. It's an invoice saying that it was paid to Micfo.

Q. In your work at StackPath, did you typically receive invoices like this one from Micfo?

A. Yes.

Q. And did you pay them?

A. Yes.

Q. Could we look at Page 5, please. This one says "unpaid," but the jury has seen bank records showing that it was in fact --

09:28 THE COURT: Do you recognize that "unpaid"? Is that your logo?

THE WITNESS: No. So that -- are you asking about the Micfo logo?

THE COURT: No. The red flag that says "unpaid," do you know what that is?

THE WITNESS: So let me explain how that works. So these providers will send us an invoice that's marked "unpaid." Once we pay it, we receive a paid version of that same exact invoice.

THE COURT: I see. So that's Micfo's flag, not yours?

THE WITNESS: Correct.

Q. And you paid these invoices, correct?

A. Yes.

Q. And this invoice is dated November 24, 2018, covering the period beginning in December, and you can see that it reflects the 104.238.37 block of IP addresses we were just looking at on the letter of authorization?

A. Yes.

Q. The letter of authorization was dated May 30?

A. Correct.

Q. Was it your practice to wait six months to get the IP address up and running?

A. No.

Q. Did you attempt to locate earlier invoices for that block of IP addresses, the 104.238.37 block?

A. Yes.

Q. Have you been able to find them?

A. I have not.

Q. Did you in fact start using that 104.238.37 block of IP addresses --

MR. NEMTSEV: Objection.

THE COURT: I haven't heard the end of the question.

Q. Did you in fact start using that 104.238.37 block of IP addresses in Boston prior to November, 2018?

MR. NEMTSEV: Objection.

THE COURT: Overruled.

A. Yes, we did.

Q. And did you pay for it prior to November of 2018?

A. Yes.

09:30 Q. Where was that IP address located?

A. Boston.

Q. How do you know that?

A. We would have been getting complaints from customers, so if you're in Boston and it wasn't there, we would see where the user experience wasn't good and someone would have complained. I never saw anything of that sort.

THE COURT: So back up. You were getting complaints from customers about what?

THE WITNESS: So using that example of why we care to

09:31 be in cities like Nashville and all that, if you were to be in Boston and had to go to Dallas to access the Internet and back, it would have been a subpar experience online, so you would have seen buffering on videos, stuff of that nature. I never saw reports of that.

Q. So you never got complaints about that?

A. No. I never saw anything.
Q. And in fact, in all your work with Micfo in all these data centers, did you ever have any concerns that the Internet addresses you directed to be placed in those centers were where they said they were?
MR. NEMTSEV: Objection.
THE COURT: Overruled. Did you ever get any complaints, period, from anyone?
THE WITNESS: As far as what the experience was like?
09:31 THE COURT: From any Boston customers?
THE WITNESS: No.
Q. Did you ever have any concerns that the IP addresses that Micfo told you were located where they were were elsewhere?
A. I never had any concerns, no.
MR. FRANK: No further questions.
CROSS-EXAMINATION BY MR. NEMTSEV:
Q. Good morning, Mr. Wall. My name is Max Nemtsev, and I represent the defendant, Mr. Klyushin, in this case. You and I have never met before, correct, sir?
09:32 A. We have never met, no.
Q. And you and I have never spoken before; is that correct?
A. We have not.
Q. You have spoken with Mr. Frank and Special Agent Hitchcock, correct?
A. Yes.

Q. Most recently on January 13, 2023; is that correct?
A. No. We met last night.
Q. You met last night? And prior to that you met at least on two other occasions; is that correct?
A. Yes.
Q. And you are accompanied by your attorney here, Ms. Walters; is that correct?
A. I am accompanied by her, yes.
Q. Are you ware, sir, that I requested to speak with you
09:33 through your attorney?
A. I am not aware of that, no.
Q. That message was never conveyed to you, sir?
A. It was not made aware to me, no.
Q. In the 2019 time frame, you worked for StackPath, correct?
A. Yes.
Q. And StackPath was sold, you testified, in March of 2019; is that correct?
A. I thought the date was April, but, yes, it was early 2019 when Ziff Davis acquired them.
09:33 Q. And StackPath leased, you testified -- well, you testified that StackPath leased the 104.238 block of IPs from Web2Objects; is that correct?
A. Yes.
Q. And you needed to lease because ARIN, the Internet registry, ran out of IP blocks to assign; is that correct?

A. They were all allocated, yes.
Q. You would agree that there's significantly more demand for IP addresses than their availability?
A. Yes.
Q. And would you agree that that requires certain customers to share IP addresses?
A. What do you mean by share them?
Q. Meaning you and I could potentially be sharing an IP; is that correct?
09:34 A. We could, yes.
Q. And IPs are portable? You can move them from one place to another at will; is that correct?
A. Yes.
Q. And you were in the business development section of StackPath; is that correct?
A. Business operations.
Q. Business operations section?
A. Yes.
Q. Did that include assembling servers, putting servers
09:34 together?
A. I had done that on occasion, but that was -- the physical putting them together and racking them was not part of my day-to-day job description, no.
Q. Your day to day was interacting with clients, dealing with customer service issues; is that correct?

A. Mostly around our growth plans, so what did we need to build to get out there, but I was not the worker that was necessarily accomplishing it.
Q. And you would agree, sir, that StackPath itself did not own any servers that were located in Boston?
A. Correct.
Q. You needed to lease the server from a company such as Micfo, correct?
A. Correct.
09:35 Q. And, sir, are you aware that Micfo was convicted of fraud that occurred between February of 2014 and the spring of 2019?
A. Yes.
Q. And that conviction does not, in your opinion, affect the -- strike that. Sir, isn't it a fact that you don't know what Micfo did with those IP addresses?
A. Can you clarify what you mean by that?
Q. You believe that Micfo took those IP addresses and placed them on their servers in Boston; is that correct?
A. I have no reason to believe that's not what they did.
09:36 Q. But you don't know for a fact. You never checked the configurations. You never went to the Markley Center down in Boston to check whether those IPs were located on the server that Micfo said they were located on; is that correct?
A. Correct.
Q. And who is Justin Boccio?

A. Justin Boccio is a systems administrator.
Q. And he is the individual that's tasked with placing IPs on certain servers; is that correct?
A. Correct. He would have been the one that would have deployed the software on the server itself.
Q. And are you aware that Mr. Boccio told the FBI that he didn't --
MR. FRANK: Objection.
THE COURT: Sustained.
09:36 Q. You testified about ARIN, correct?
A. I said who they were, yeah.
Q. Can we pull up Exhibit 176.
THE CLERK: I switched.
MR. NEMTSEV: Thank you, Maryellen.
THE CLERK: You're welcome.
Q. Does this appear to be a registration record for the 104.238 IP addresses for the time period between May 18, 2018 and September 30, 2020?
A. Yes.
09:37 Q. Could we please turn to Page 2.
MR. NEMTSEV: Ms. Lewis, could you please assist?
THE CLERK: Do you want me to switch over?
MR. NEMTSEV: Yes, please.
THE CLERK: Okay, not a problem. Hold on. Okay.
Q. And this is Page 2 of the same record, and it says that

Web2Objects reassigned 104.238 -- I just lost my -- reassigned 104.238 to the filing organization, and it lists "Strong Technology LLC." Do you see that?

A. Yes.

Q. And Strong Technology LLC is one of the companies that you testified to was a subsidiary of StackPath; is that correct?

A. That is correct.

Q. And specifically Strong Technology operated the VPN, StrongVPN; is that correct?

09:38 A. So IP addresses, even if they were assigned to Strong Technology, could in theory been used by any of the subsidiaries.

Q. Well, in this instance, this IP address, this IP range was specifically assigned and designated to the Strong Technology LLC company, correct?

A. The LLC, yes.

Q. And StrongVPN, to your knowledge, never offered an IP server or a server in Boston, correct?

A. Strong had servers in Boston, yes.

Q. As part of your operation of StrongVPN, IPVanish, and

09:39 other companies, you have websites, correct?

A. Yes.

Q. And those websites have status pages, do they not?

A. They do.

Q. And on those status pages, you show which servers are available at what time; is that correct?

A. I think the only one that had automated status pages in the account portal was IPVanish. The rest of them, I could be mistaken, but I don't believe that they did.

Q. Well, would you agree that it's important to update the status pages in order to give your clients accurate information as to what servers were available and which ones were not?

A. Yes, I would believe that it would be important to put an emphasis on that, yes.

Q. So you would imagine that -- or do you believe that the

09:39 status pages for StrongVPN are accurate?

A. We -- I don't know back at that time.

Q. You worked for StackPath back at that time, correct?

A. I did. Strong was not a brand that we focused much on. The flagship brand was IPVanish.

Q. And you were consumer-facing, correct?

A. Yes.

Q. You dealt with customers and their complaints, correct?

A. Yes.

Q. Did you ever hear a customer tell you that what was

09:40 located on the StrongVPN page in terms of servers and status was inaccurate?

A. Inaccurate in what sense?

Q. In the sense that some certain servers were unavailable, other servers were available, but not on the list.

A. So in the client application, a server would not show up

unless it was online. So in the client app, that would be one thing, but the website was manual in that respect.

Q. And how frequently is the website updated, if you know?

A. When we would add cities, it would be a matter of getting with the marketing team to let them know to add it, and then however long that process took. It could take weeks.

Q. It could take weeks, but it wouldn't take months or six months, correct?

MR. FRANK: Objection. Calls for speculation.

09:41 THE COURT: If you know.

A. I don't know in that case.

Q. It's important for your marketing purposes to have accurate lists of available servers, correct?

MR. FRANK: Objection. Asked and answered.

THE COURT: Sustained.

Q. Are you familiar with the website Wayback Machine?

A. Yes.

Q. And what is it?

A. They take snapshots of Internet, like, websites, and then

09:41 you can go back to them to see what they look like on a historical date.

MR. NEMTSEV: And could we pull up Exhibit 412, please.

MR. FRANK: Objection. Hearsay and lack of authenticity.

THE COURT: Well, don't pull it up until he sees it.
MR. FRANK: Your Honor, I object to this being displayed.
THE COURT: I don't know. It can't be put up on the screen until you --
MR. KOSTO: It was just put up on the screen, your Honor.
THE COURT: For a nanosecond.
Q. And, sir, you testified that you searched for invoices from Micfo prior to December of 2018 related to this IP block; is that correct?
A. Yes.
Q. And you were not able to locate any invoice that references this IP block at a time earlier than December of 2018; is that correct?
A. I believe that to be correct, yes.
Q. Sir, did you locate any other invoices that referenced the same server that you were leasing from Micfo indicating that they were assigned to a different IP range?
A. I didn't. All I did was look for Micfo invoices, and I sent those along. I didn't pay much attention to them. You'd have to be more specific.
MR. NEMTSEV: Could we pull up Exhibit 416, which is in evidence.
Q. Is this one of the invoices that you provided to the

government in response to their subpoena?
A. Whether I provided it, I'm not entirely sure, but it looks like a Micfo invoice just like the rest of them.
Q. Micfo invoice, this one is marked "paid," is that correct?
A. Yes.
Q. Invoice date is October 25, 2018; is that correct?
A. Yes.
Q. The first item that you're being invoiced for is $415 for leasing the Server 07 and assigning it to the IPs
09:44 104.156.206.2; is that correct?
A. Yes.
Q. And that is not the same as the 104.238 IP address that the government requested you to look for, correct?
A. So the way that that works is, in order to get the server set up, they provided a set of IPs, a smaller block. So slash 27 in this instance is 32 IP addresses, which is insufficient for us to provide the services to our end-users. And then we would go and provide a larger block that we leased out, so you could have both blocks living on that same exact server.
09:45 Q. But you don't know in this instance, or based on this invoice, that both blocks were on that server; is that correct?
A. On that invoice, there's nothing that states it. I would agree.
Q. And, sir, does any StackPath affiliate provide free services, free VPN services?

A. That specific time frame that we're talking about? I do not believe so, but I cannot be for certain.
Q. And you would agree that, in order to use a VPN service, you would have to sign up with your company StackPath?
A. One of the subsidiaries, yes.
Q. It's either IPVanish or StrongVPN or any other subsidiary, correct?
A. Correct.
Q. And in order to sign up, you would have to take a name, an
09:45 address, a credit card; is that correct?
A. Yes.
Q. And how much does the service cost, sir?
A. Back then, somewhere between $10 a month and $60 a year.
Q. Did you ever locate any account records belonging to Mr. Klyushin, or Mr. Ivan Ermakov, or Mr. Nikolai Rumiantcev?
A. My interaction with the requests that were from the government, they never asked. I was never a part of that part.
THE COURT: Say that again?
THE WITNESS: I personally was never asked to look up
09:46 any customer records myself, so I don't know what was provided.
Q. And, sir, do you know what IP geolocation is?
A. Yes.
Q. And in the VPN business, IP geolocation is important, correct?
MR. FRANK: I object, and this is beyond the scope.

THE COURT: Overruled.
A. Yes, it is confusing. Say, for example, you went to connect to a server in Boston, and I think there was a document from Web2Objects where their corporate address was in New York City, so it probably looked like New York City. And then you go to Google Maps, and it thinks you're in New York City. You try to correct for that.
Q. You try to correct for it. And specifically in VPNs, when you tell a customer that you are connecting, for example, to a
09:47 Dallas server, they expect everyone else that looks at their IP to believe that they're from Dallas, Texas?
MR. FRANK: Objection to what other people expect.
THE COURT: Sustained, sustained.
Q. Isn't it important to get IP geolocation correct in connection with VPN IP addresses?
MR. FRANK: Objection.
THE COURT: Sustained.
THE WITNESS: Yes.
THE COURT: So don't answer when I say "sustained."
09:47 THE WITNESS: Sorry.
MR. FRANK: Move to strike.
THE COURT: I strike it.
MR. NEMTSEV: Nothing further, your Honor.
THE COURT: Anything?
MR. FRANK: Briefly, your Honor.

REDIRECT EXAMINATION BY MR. FRANK:

Q. Mr. Wall, you can have multiple blocks of IP addresses on the same server, correct?

A. Yes.

Q. Were you absolutely meticulous about maintaining all your invoices that you paid back in 2018?

A. No.

Q. The 104.238.37 IP address block that we've been talking about, was it in Boston in 2018?

09:48 A. Yes.

MR. FRANK: No further questions.

THE COURT: Okay, thank you.

Anything else?

MR. NEMTSEV: Nothing further, your Honor.

THE COURT: You can leave, unless you want to stay.

THE WITNESS: No. I'm good.

(Witness excused.)

MR. KOSTO: The United States calls Aditi Shah.

ADITI SHAH

09:49 having been first duly sworn, was examined and testified as follows:

THE CLERK: You can be seated. Could you please state and then spell your last name for the record.

THE WITNESS: My name is Aditi Shah, and the last name is S-h-a-h. Aditi, A-d-i-t-i.

DIRECT EXAMINATION BY MR. KOSTO:

Q. Good morning, Ms. Shah.

A. Good morning.

Q. Go ahead and pull that microphone nice and close so we can all hear you. I'll do my best to keep my voice up, and I'd ask you to do the same. Okay?

A. Okay.

Q. What city do you work in now, Ms. Shah?

A. I work in Raleigh.

09:50 Q. And what company do you work for today?

A. Today I work for The Select Group, and I work as a contractor with Cisco, and I am a contractor with Bank of America.

Q. And what does your contract with those companies involve?

A. I work as a senior network engineer for the data center.

Q. Whose data centers?

A. Bank of America's data centers.

Q. Let me take you back in time to the period between June of 2017 and February of 2019. Were you working as a network

09:50 engineer somewhere else?

A. Yes.

Q. And what was the name of the company you worked at back then?

A. I was working with Micfo. It was based in Charleston.

Q. South Carolina?

A. Yes.
Q. And we've heard both Mikefo (Phon) and Micfo. What's right?
A. Mikefo (Phon) is the correct pronunciation.
Q. And what was your job title at Micfo?
A. I was still a network engineer with Micfo.
THE COURT: I can't understand what you're saying. Slow down.
THE WITNESS: I was working as a network engineer at Micfo.
09:51
THE COURT: As a network engineer?
THE WITNESS: Yes, ma'am.
Q. As a network engineer at Micfo, did your job responsibilities include assigning IP addresses --
MR. NEMTSEV: Objection, your Honor.
THE COURT: Overruled.
Q. Did your job responsibilities include assigning IP addresses to Micfo data centers around the country?
A. Yes, sir. That was part of my job duties.
09:51
Q. Let me direct your attention to Government's Exhibit 267 in evidence and the last page of that exhibit.
Thank you, Ms. Lewis.
I'm showing you the last page of 267. Do you recognize it?
A. So this is one of the letters that we would normally

receive, like a letter of authorization we would receive from our clients.

Q. And what is a letter of authorization from your time at Micfo?

A. A letter of authorization is required when we are asked to use or announce a certain IP which doesn't belong to Micfo to our ISP provider. So we need the proof that that IP belongs to whoever is asking us to use it.

Q. So in the case of Exhibit 267, who did the IP address belong to? Who was the authorizing company?

A. In this case, it was the Web2Objects LLC.

Q. And who was the letter of authorization authorizing to use the IP addresses in this document?

A. It authorizes Micfo.

Q. And can I have you read the first IP block that is referenced in the group of them there in the third paragraph.

A. Sure. It's "104.238.37.0/24, Boston."

Q. And what city was listed for that IP?

A. Boston.

Q. How many cities in total were listed in this letter of authorization?

A. Seven.

Q. That's Boston, Cleveland, Denver, Milwaukee, Nashville --

A. Salt Lake City.

Q. -- and St. Louis?

A. Yes.
Q. And were any of these any different than any of the others for your purposes?
A. No.
Q. When you received a letter of authorization like this one from Web2Objects, what would you do with it?
A. So this is essentially telling Micfo that we want these IPs to be announced in these locations so that we can use them on our servers, and Micfo was an infrastructure service
09:54 provider, so we did provide those servers as well.
Q. Where would you send this letter of authorization when you received one?
A. We would send it to our ISP providers in each location so that they can announce these.
Q. First of all, what is announce?
A. So announcement --
MR. NEMTSEV: Objection, your Honor.
THE COURT: Well, we're going to stick to the documents.
MR. KOSTO: Sure.
09:54 Q. Who was the ISP provider for Boston?
A. We had multiple providers in most of our locations. We were in multihomed -- that is, we had two ISP providers a case -- and in Boston we had, as far as I remember, we had Cogent and GTT.
Q. So what did you do with the letter of authorization --

what's the date on the letter of authorization?
A. It's May 30, 2018.
Q. And can I take you, please, to Page 6 of Exhibit 267 with Ms. Lewis' help.
MR. KOSTO: Ms. Lewis, can you highlight the bottom two-thirds of the page.
Q. Do you see the date on this blown-up part of the document?
A. Yes.
Q. What is it?
09:55 A. It's May 30, 2018.
Q. Is that the date on the letter of authorization?
A. Yes.
Q. And who did you send it to?
A. Cogent.
Q. And what was Cogent again?
A. Cogent is an ISP provider, upstream provider. So once we send the data to Cogent, it would be uploaded on the internet; they can accept the traffic from these IPs.
MR. NEMTSEV: Objection, your Honor.
09:55 THE WITNESS: I'm sorry.
Q. What did you ask Cogent to do?
THE COURT: I'm having trouble following, so hold on.
MR. KOSTO: May I proceed, your Honor?
THE COURT: I'm not sure what she said, and it's not clear on here either, so I am not sure what I am striking or

not, so this is important to you.
Q. Let me go back one step. Ms. Shah, did you send this email to Cogent?
A. Yes, I did.
Q. And in this email, do you see the first IPv4 prefix listed in bold?
A. Yes.
Q. Could you read it.
A. "104.238.37.0/24."
09:56 Q. Did this email also include instructions for other cities?
MR. NEMTSEV: Objection.
THE COURT: I haven't heard the question. I'm looking at the email. We're all looking at the email. What's the question?
Q. Could you read the next city on the exhibit.
A. Cleveland.
Q. And is there a different IP for Cleveland?
A. Yes, sir.
Q. Is there another city beneath that one?
09:56 A. Yes, sir, Denver.
Q. And is there a different IP beneath that one?
A. Yes, sir.
Q. And to the next page, please, Ms. Lewis. Is there another city, Milwaukee, underneath that one?
A. Yes, sir.

Q. And is there another city underneath that one, St. Louis?
A. Yes, sir.
Q. What did you ask Cogent to do in this email?
A. To accept --
MR. NEMTSEV: Objection.
THE COURT: Overruled.
A. To accept traffic from the IP prefix mentioned in this email.
Q. Let me take you to Page 1 of Exhibit 267. Do you see the
09:57 date in the upper left-hand corner of this email?
A. Yes, sir.
Q. Is that May 30th?
A. May 30th, 2018.
Q. Is it the same day as the letter of authorization?
A. Yes, sir.
Q. Is it the same day that you e-mailed Cogent requesting them to add Boston?
A. Yes, sir.
Q. And could you read Cogent's reply, the "Dear Cogent
09:57 Customer" and the first sentence.
A. Sure. "Dear Cogent customer: Your BGP prefix-list addition has been completed."
Q. What does it mean, "your BGP prefix-list has been completed"?
A. BGP is a routing protocol, so we --

THE COURT: Is a what?
THE WITNESS: A routing protocol.
THE COURT: All right.
A. So basically that's the way Micfo and Cogent communicated was in that protocol, and based on that protocol, this IP would be now accepted by Cogent to allow traffic to and from these IPs.
Q. And what did you do in response to this email? What was your practice when you received this email back?
09:58 MR. NEMTSEV: Objection.
THE COURT: Sustained.
Q. Okay. Did you ever receive any complaints from your customer that the IP addresses you sent this day were not working as intended?
MR. NEMTSEV: Objection.
THE COURT: Sustained.
Q. Did you hear anything from your customer --
THE COURT: Remember, limited to the documents.
Q. Did you receive any other communications from Cogent?
09:59 A. We would have, but it depends on the date and time related to what.
MR. KOSTO: No further questions, your Honor.
MR. NEMTSEV: Your Honor, could I be seen at sidebar for a second?
THE COURT: Sure.

MR. NEMTSEV: Thank you.

SIDEBAR CONFERENCE:

MR. NEMTSEV: Based on the representations in my opening that there's going to be no Micfo witness, would your Honor consider giving an instruction that, you know, it's not because I lied to the jury. It's because they just identified this witness and gave us no notice before the start of trial?

THE COURT: Yes, I will do that to cure that. I'll give a curative instruction.

10:00 This is somebody you just found, right?

MR. FRANK: Yes.

MR. KOSTO: In response to the defense case.

THE COURT: Well, it's your case, but nonetheless I think she's useful, if you can understand the accent. But I did limit the government to specifically the document we're all familiar with, so, okay.

MR. NEMTSEV: We're not going to ask --

THE COURT: You're not going to cross at all?

MR. NEMTSEV: No.

10:00 THE COURT: All right.

(End of sidebar conference.)

MR. NEMTSEV: Maybe a couple questions, your Honor.

THE COURT: I knew it.

I should have done this before. This has been a newly named witness because someone who's recently found, basically.

So does anyone know her? I didn't have her on the witness list, and the defense didn't find out about her before trial, so I just wanted -- it's part of this chain in trying to understand things. So does anyone know her? Okay, that's fine. Okay, thank you.

CROSS-EXAMINATION BY MR. NEMTSEV:

Q. Good morning, Ms. Shah.

A. Good morning.

Q. You and I have never met, correct?

10:01 A. Yes, never.

Q. The first time the government contacted you was sometime last week; is that correct?

A. That's correct.

Q. And never before have you spoken to anyone, correct?

A. No.

Q. And they sought your testimony through a subpoena; is that correct?

A. Yes.

Q. And they brought you here over the weekend, correct?

10:01 A. Yes, sir.

Q. How long have you been in Boston?

A. I have been just one day.

MR. NEMTSEV: Nothing further.

THE COURT: Thank you.

MR. KOSTO: Nothing, your Honor. Thank you.

THE COURT: Thank you. Sorry you had to stay.

(Witness excused.)

MR. KOSTO: Your Honor, the government calls Karyn Yanochko.

KARYN YANOCHKO

having been first duly sworn, was examined and testified as follows:

THE CLERK: Could you please state and spell your last name.

10:02 THE WITNESS: Sure. My name is Karyn Yanochko, spelled K-a-r-y-n. Last name is spelled Y-a-n-o-c-h-k-o.

DIRECT EXAMINATION BY MR. KOSTO:

Q. Good morning, Ms. Yanochko.

A. Good morning.

Q. Would you please bend that microphone up so we can all here you.

A. Sure.

Q. Try one more time, just your first and last name.

A. Karyn Yanochko.

10:02 MR. KOSTO: Can everyone hear?

Q. Where do you work, Ms. Yanochko?

A. I work at the United States Attorney's Office here in the District of Massachusetts.

Q. What's your job title at the U.S. Attorney's Office?

A. I am a financial investigator.

Q. Are you a federal agent?
A. I am not.
Q. Are you a law enforcement agent?
A. No.
Q. How long have you been a financial investigator?
A. It will be two years in April.
Q. And can you briefly describe to the jury what it is you do.
A. I work with prosecutors and special agents reviewing financial documents such as bank statements, wire transfers; also the supporting documentation like IP log-ins. I summarize that information and I create charts.
Q. You sometimes testify at trials?
A. I do.
Q. Where did you work before joining the U.S. Attorney's Office?
A. I was a contract auditor for the Department of Defense for seven years.
Q. What did you do there?
A. I analyzed and audited voluminous data which supports the cost of major defense contracts.
Q. Big numbers, I assume?
A. Lots of numbers.
Q. What's your educational background?
A. I have a bachelor's degree in accounting from Keystone

College and a master's of business administration from the University of Hartford.

Q. Do you hold any professional certifications?

A. Yes. I'm a Certified Fraud Examiner.

Q. What's your involvement in this case specifically?

A. So I was asked by the prosecutors to review the downloads, the information from Donnelly Financial from the ActiveDisclosure.

Q. And what did you do after analyzing that information in general terms?

A. I created a series of summary charts.

Q. And which programs logs did you look at?

A. The program was called the ActiveDisclosure from Donnelly Financial.

Q. And how much data was in those logs?

A. Millions of lines of data.

Q. And so which specific lines of data were you focused on in your analysis?

A. The download.ASPX.

Q. And what kind of data did you analyze and summarize from those download commands?

A. So I summarized information for the download command lines on the date, the time, the client, and the downloads, and the IPs.

Q. How about the name of the document that was downloaded?

A. As well as that.
Q. And when you said IPs, just clarify. What IP address were you summarizing?
A. I was summarizing the IP addresses that I was directed to by the prosecutors.
Q. Were those the IP addresses that connected to Donnelly Financial?
A. Yes.
Q. The ones that downloaded the documents?
10:05 A. Yes.
Q. Okay. What period of time did the logs that you looked at from Donnelly Financial cover?
A. From February, 2018, through November of 2020.
Q. And how did you narrow down the information? What was the mechanism of sorting through all the rows?
A. Sure. I used Excel and a series of filters and formulas.
Q. Microsoft Excel?
A. Yes.
Q. And you made charts to present your summaries to the jury?
10:06 A. Yes.
Q. Let me show you Government's Exhibit 190, and I'd offer it.
(Exhibit 190 received in evidence.)
Q. Do you recognize the exhibit?
A. Yes.

Q. Did you prepare and verify it?
A. I did.
Q. And what is it?
A. This is a chart that I prepared from the Donnelly Financial ActiveDisclosure download data, specifically for the download.ASPX command line, for the username RR52260 associated with Julie Soma's account, for the IP address 89.238.166.235 for October of 2019.
Q. So was this all of the downloads that took place over the
10:06 IP address in blue contained within the dataset?
A. For October, 2019.
Q. And if we wanted to go back and check your chart for its accuracy, where would we go?
A. You would look up the Donnelly Financial ActiveDisclosure data.
Q. Let me show you Government's Exhibit 71K in evidence.
MR. KOSTO: And if we could have 190 on the left, please, Ms. Lewis.
Q. So do you recognize 71K on the left?
10:07 A. Yes.
Q. What is that?
A. So this is the raw data from the Donnelly Financial ActiveDisclosure.
Q. So what's the date and time in the raw data?
A. Date and time is October 23, 2019, at 10:17.

Q. And what is the time reflected on the first line, first row of your chart?
A. The date and time is October 23, 2019, at 10:17 Zulu.
Q. What's the IP address in the raw data on the left, 71K?
A. Is 89.238.166.235.
Q. And where do you see that on Exhibit 190?
A. That is in the header.
Q. And do you recognize any usernames in the raw data on the left?
10:07 A. I do.
Q. Where is it?
A. On the left, it is RR52260.
Q. And that's your summary?
A. And that is also my summary.
Q. And do you recognize the name of the client reflected in the raw data?
A. Yes.
Q. And what is it?
A. Tesla.
10:08 Q. And is that what appears on your summary?
A. Yes.
Q. And does the name of the document match as well?
A. Yes.
Q. Okay. Did you do this analysis for a number of different IP addresses that you were requested to look at?

A. Yes.
Q. And were many of them tied to Julie Soma's account?
A. Yes.
MR. KOSTO: Before we leave that, Ms. Lewis has suggested that I offer 71K. Thank you.
(Exhibit 71K received in evidence.)
Q. Let's look at Exhibit 191, please. Is this a multipage document?
A. Yes.
10:08 Q. What are you summarizing here?
A. Here I am summarizing the download.ASPX information from the Donnelly Financial ActiveDisclosure for the username associated with Julie Soma for the --
Q. I'm sorry. What's the IP address? You were right ahead of me there.
A. The IP block is 104.238.37 for the period of October, 2018, through November, 2018.
MR. KOSTO: Ms. Lewis, can you quickly show Ms. Yanochko the number of pages in the document.
10:09 Q. How many did you see there, Ms. Yanochko?
A. Four pages.
Q. Approximately how many downloads were there reflected in these pages?
A. There's about 113.
Q. And I'd ask you on Page 1, please, from the middle of the

page starting with "Capstead," could you please read aloud the companies that are listed in order. You can skip the duplicates.

A. Capstead Mortgage Corporation, Essendant Incorporated, Getty Realty Corporation, Microsoft Corporation, Prosperity Bank Shares Incorporated, Packaging Corporation of America, Stepan Company, Altra Industrial Motion Corporation, Aquila Corporation, PGC Partners Incorporated.

Q. Let me stop you there. Do you notice anything about those company names?

A. They're alphabetical.

Q. Did you alphabetize them?

A. No.

Q. What is the order that this information is presented in?

A. It is presented chronologically.

Q. And so what's the approximate amount of time that these downloads took place in these company names?

A. It's approximately an hour.

Q. Let me direct you to Exhibit 176. Can you please read aloud on Page 2 the IP block referenced in the first sentence.

A. 104.238.37.

Q. And what's the entry for city and state reflected in 176?

A. Boston, Massachusetts.

Q. Okay. Let me direct your attention to Exhibit -- and that's the IP address that was on the chart we just looked at?

A. Yes.
Q. Let me direct your attention to Exhibit 192. Do you have it there?
A. Uh-huh.
Q. Do you recognize it?
A. Yes.
Q. And what does it summarize?
A. This is another chart that I created based off the Donnelly Financial ActiveDisclosure data, also summarizing the
10:11 downloads for the username associated with Julie Soma for the IP address listed in the header for November 6, 2019, through November 8, 2019.
Q. Can I have you read the third row in relation to Roku Inc. and tell the jury what it's summarizing.
A. Sure. It is on November 6, 2019, at 12:54 Zulu and 4:54 a.m., the Exhibit 99.1 document was downloaded for the company Roku Incorporated.
Q. Over Julie Soma's username?
A. Over Julie Soma's username.
10:12 Q. And did you make a time conversion in connection with your summary here?
A. I did.
Q. What's the 4:54:49 seconds time?
A. That is the Pacific Time.
Q. Okay, let's move to Exhibit 193. I'll ask you if you

recognize it.
A. Yes, I recognize it.
Q. It's fair to say it's another download summary for the IP address in blue there?
A. Yes.
Q. Does it concern February 5, 2018?
A. It does.
Q. And it's again on Ms. Soma's account?
A. Yes.
10:12 Q. Let me have you read and summarize for the jury the fourth and fifth rows in relation to Snap Inc.
A. Sure. On February 5, 2018, between 7:16 and 7:18 Zulu, or 11:16 p.m. and 11:18 p.m., the documents Exhibit 99.1 and Snap Master were downloaded for Snap Incorporated.
MR. KOSTO: Ms. Molloy, I'd offer 190, 191, 192, 193 and just to get ahead of ourselves, 194 and 195 in case I forget.
(Exhibits 190-195 received in evidence.)
Q. And can you read and convert the time of these downloads
10:13 for the jury in rows 4 and 5.
A. Sure. It's 7:16 and 7:18 in Zulu time and 11:16 and 11:18 in Pacific.
Q. Let's move to the recently offered 194. Is this download activity over Ms. Soma's account?
A. Yes.

Q. Is it for the IP address in blue?
A. Yes.
Q. What time period does it cover?
A. For July, 2019.
Q. Can I have you read and summarize the fifth row only. Start with the document that was downloaded.
A. So the 99.1 document was downloaded.
Q. What company?
A. For SS&C Technologies Holdings Incorporated.
10:14 Q. And what time of day or night Pacific Time?
A. It's 10:09 a.m.
Q. Okay. Could I also please have you read the company list down from Atlas Air. You can skip any duplicates.
A. Atlas Air Worldwide Holdings, Inc., Abiomed incorporated, Apartment Investment and Management Company, British American Tobacco PRC, Chemours Company, Coherus Bioscience Incorporated.
Q. I'll stop you there. What, if anything, do you notice about the order of the companies?
A. They're alphabetical.
10:14 Q. Let's move to Exhibit 195. I believe it's been offered. Is this another of your summaries?
A. Yes.
Q. Does it date to May, 2019, concerning the IP address in blue?
A. Yes.

Q. Over Ms. Soma's account?
A. Yes.
Q. These are all downloads at that time?
A. Yes.
Q. And can I have you please read the entry related to Kohl's Corporation about midway down the page.
A. On May 20, 2019, at 12:29 Zulu, or 5:29 a.m. Pacific, the Exhibit 99.1 document was downloaded for Kohl's Corporation.
MR. KOSTO: Let's move, please, to Exhibit 195A, and, Ms. Lewis, I'd offer it.
(Exhibit 195A received in evidence.)
Q. What's the IP address for this summary, Ms. Yanochko?
A. 119.204.194.11.
Q. Approximately how many downloads are there in May, 2019, for this IP address?
A. Approximately ten.
Q. Please read the row the fourth from the bottom.
A. On May 9, 2018, at 7:48 Zulu, or 12:48 a.m., the HVNP master document was downloaded for Horizon Pharma PLC.
Q. What time is that on the West Coast of the United States?
A. That's 12:48 a.m.
MR. KOSTO: Let's move to Exhibit 195D, please, and I'd offer it.
Just a few more, Ms. Yanochko.
(Exhibit 195D received in evidence.)

Q. What is this one?
A. Another document that I created from that Donnelly Financial ActiveDisclosure data.
Q. Could you read the IP address, please.
A. Sure. It's 199.249.230.42.
Q. What's the date?
A. On October 11, 2019.
Q. What's the Pacific Time range?
A. The Pacific time range is 5:01 a.m. through 5:11 a.m.
10:16 Q. And what are the last three documents that were downloaded for Sleep Number, Alcoa, and M&T Bank?
A. EX99.1, EX99.1, and Exhibit 99.1.
MR. KOSTO: Let's move to Exhibit 195F, please, and I'd offer it.
(Exhibit 195F received in evidence.)
Q. This one looks a little bit different, Ms. Yanochko; is that correct?
A. Yes, but it's from the same download information from Donnelly Financial.
10:17 Q. And which IP address does this concern? I don't see any listed in the title.
A. So for this chart, I've used all of the IP addresses associated with the username RR522 for Julie Soma, excluding the Donnelly Financial home office VPN IP address.
Q. You said you excluded the home office VPN?

A. Yes.
Q. Okay. Approximately how many downloads were there in this dataset that you're summarizing here?
A. For this graph, there's about 2,300 accounts.
Q. All over the Soma account?
A. All over the Soma account.
Q. And how are you showing them on this exhibit in particular? This one's a little new.
A. So this one, I grouped them by hour.
10:18 Q. And how did you do that? Let's say there was downloaded at 12:30 in the afternoon, where would that fit in your chart?
A. So that would fall under the 12:00 p.m. hour.
Q. And how about 10:45 p.m., even though it's close to 11:00 p.m.?
A. It would still fall under 10:00 p.m.
Q. So you rounded down essentially?
A. I just used the hour.
Q. That's a better way of saying it. Thank you. What was the time period reflected on your summary where the smallest
10:18 number of downloads occurred?
A. Between 3:00 p.m. and 8:00 p.m.
Q. And what time zone are we in here?
A. This is in the Pacific Time zone.
Q. What was the timing of the period of the day when the largest number of downloads appeared to take place over

Ms. Soma's account?
A. 5:00 a.m.
MR. KOSTO: Let's move to Government's Exhibit 195F on the left, please, and 195E on the right. And I'd offer 195E and 195F if I haven't.
(Exhibit 195E received in evidence.)
Q. So we've added 195E. Is that another summary you prepared?
A. Yes.
Q. How does it relate to 195F?
10:19 A. So it's the same information from 195F, then translated into Moscow Standard Time.
Q. And how far ahead of Universal Zulu Time is Moscow Standard Time?
A. So from Zulu to Moscow, it's three hours ahead.
Q. In 195E, what is the time when the least downloads appear to take place over Ms. Soma's account?
A. Between 1:00 a.m. and 7:00 a.m.
Q. And what is the time period where the most downloads appear to take place over Ms. Soma's account?
10:19 A. 4:00 p.m.
Q. And so, again, what is the relationship between the data summarized in 195E Moscow time and 195F Pacific Time?
A. So it's the same information, just shifted for the time zone.
MR. KOSTO: Let's move to Exhibit 195B, and I'd offer

it.

(Exhibit 195B received in evidence.)

Q. What are you summarizing in 195B?

A. It's the ActiveDisclosure download information, but this time it summarizes the information for the username associated with Hyeyoung Han for the IP addresses listed above.

Q. And there are three there?

A. And there are three.

Q. Could I have you read the middle one.

10:20 A. It is 199.249.223.130.

Q. And what's the time period?

A. From October 28, 2019, through April 30, 2020.

Q. Does this chart work the same way as the one you prepared for Ms. Soma's downloads?

A. Yes.

Q. Everything rounded down to the hour?

A. Yes.

Q. And what time zone is this one set in?

A. So this one is set in Korean Standard Time.

10:20 Q. And how many downloads, just to illustrate, were there between, say, 7:00 and 8:00 p.m.?

A. About 120.

Q. And what about noon Korea time?

A. Zero.

Q. 3:00 p.m. Korean time?

A. Zero.
Q. Did you allow for Daylight Savings Time in this chart?
A. So Korean Standard Time doesn't observe Daylight Savings.
MR. KOSTO: Let's add, please, Ms. Lewis, and I'd offer Government Exhibit 195C alongside 195B.
(Exhibit 195C received in evidence.)
Q. What is 195C?
A. It's the same chart as 195B but now in Moscow Standard Time.
10:21 Q. And what's the time difference between Moscow Standard and Korea Standard?
A. Six hours.
Q. And in Moscow Standard Time, what is the range of hours in which the largest number of downloads occurred?
A. Between 1:00 p.m. and 5:00 p.m.
Q. And the smallest number of downloads in Moscow Standard Time?
A. 11:00 p.m. through 9:00 a.m.
Q. Let me show you Government's Exhibit 195H, please.
10:22 A. So another chart that I created based on the Donnelly Financial download data, but this time just for the one specific IP address listed above for the account associated with Julie Soma's username.
Q. Could I have you read the IP address aloud in blue.
A. Sure. It's 64.42.179.159.

Q. And what's the time period?
A. From October 24, 2019, through November 26, 2019.
Q. Approximately how many downloads were there in this dataset?
A. Approximately 120.
Q. When do all of them take place Pacific Time?
A. They all take place between 1:00 a.m. and 7:00 a.m.
Q. I'm showing you Government's Exhibit 195G. How does 195G relate to 195H?
10:23 MR. KOSTO: I'd offer both H and G, Ms. Molloy. I'm sorry.
(Exhibits 195H and 195G received in evidence.)
A. So this is the same chart as 195H, but the previous chart just shifted into Moscow Standard Time.
Q. Are the downloads between 12:00 and 6:00 in the afternoon Moscow Standard Time?
A. Yes.
Q. Let's move to Government Exhibit 195I. I think this is our last one, Ms. Yanochko.
10:23 THE COURT: This is the last --
MR. KOSTO: This is the last summary chart.
THE COURT: -- with this witness?
MR. KOSTO: Yes, it is. I'm sorry, your Honor. What is the question?
THE COURT: This is the last exhibit with this

witness?

MR. KOSTO: It is.

THE COURT: Are you done with the witness?

MR. KOSTO: Yes. I'd like to ask her about this chart, and then we'll be done with this witness.

THE COURT: Thank you. I'm just -- Ms. Molloy needs to go somewhere, so we'll switch out with Clary, and I just want to make sure that we're getting all the exhibits in.

MR. KOSTO: Would the Court like to pause for a minute now and stretch, or should we keep going?

10:23

THE COURT: No. Just finish this witness. Are you going to have cross with her?

MR. NEMTSEV: I will, your Honor.

THE COURT: Do you need the charts to come back up again?

MR. NEMTSEV: Potentially, yes. At least one or two.

THE COURT: Okay, so if you're --

Okay, Clary can do this. I just wanted to make sure.

MR. KOSTO: We'll leave it with Ms. Lewis and she'll be able to help, as well.

10:24

THE COURT: Okay, thank you. I'm sure Clary can do it as well. I just want to make sure we don't -- this is seamless.

MR. KOSTO: Even though Ms. Molloy just got up, I'm going to offer 195I. Sorry, Ms. Molloy.

(Exhibit 195I received in evidence.)

Q. This is a slightly different-looking summary. Did you prepare this one?

A. I did.

Q. And so help us understand what you did here. What is this summary?

A. So this summary summarizes all of the Donnelly Financial ActiveDisclosure download data for -- all the download data excluding the IP address associated with the Donnelly Financial VPN, and then I grouped them by month for this chart, and each of these were assigned a color.

Q. Who asked you to exclude the Donnelly Financial corporate VPN?

A. The prosecutors.

Q. And what are the last names of the five users whose downloads you're summarizing here?

A. Soma, Han, Gray, Lewis, Gebremariam.

Q. And what are the percentages in the box, the lower box?

A. The percentages represent how much of this dataset those usernames represented.

Q. So how many downloads are in this dataset?

A. Approximately 2,900.

Q. So when you say 80 percent in parentheses next to Ms. Soma, how many of the 2,900, approximately, was her account responsible for?

A. Approximately 2,300.
Q. Okay. And what is the up-down axis on this chart, if the time goes from left to right, month by month?
A. It's the number of downloads.
Q. And from the period February of 2018 through November or December of 2020, what is the primary color there?
A. Blue for Julie Soma.
Q. And then what does it shift to in January, February, March, and April?
10:26 A. It shifts to red.
Q. And who is red?
A. That would be Hyeyoung Han.
Q. And in May, what does it shift from and to?
A. It shifts to blue for Lewis.
Q. Would you agree with me that that's purple?
A. Sorry. Purple.
Q. Or purplish. And then on to green and on to aquamarine?
A. Yes.
MR. KOSTO: May I have one moment, your Honor.
10:27 (Discussion between government attorneys.)
MR. KOSTO: Nothing further, your Honor.
THE COURT: Okay.
CROSS-EXAMINATION BY MR. NEMTSEV:
Q. Good morning, Ms. Yanochko.
A. Good morning.

Q. My name is Max Nemtsev --

THE COURT: Uh-uh.

MR. NEMTSEV: Louder or slower?

THE COURT: Louder, louder.

MR. NEMTSEV: All right. Thank you, Judge.

Q. You and I have never met before, correct?

A. That is correct.

Q. We've never spoken before, correct?

A. That is correct.

10:27 Q. Have you been watching the trial as it goes along?

A. I have not.

Q. And you prepared these analyses and these summary charts at the request of the prosecutors in this case, Mr. Kosto and Mr. Frank?

A. Yes.

Q. And they provided you with the information necessary to create these charts; is that correct?

A. The information was provided through them.

Q. And they provided to you what they want to see in these

10:28 charts, correct?

A. Yes.

Q. They told you, for example, to limit your analysis to the download at ASPX; is that correct?

A. Yes.

Q. And they told you to convert PST to, for example, Moscow

Central Time, correct?
A. Yes.
Q. And you have no knowledge whether anything happened in Moscow, correct?
A. I don't have any knowledge of anything that would indicate why the time zones would be one or another, no.
Q. This was just at the request of the prosecutors, correct?
A. Yes.
Q. And you would agree that in UTC+3, there's significantly more countries and significantly more cities than just Moscow or Russia?
A. I'm actually not sure exactly what falls into 3.
Q. If I represent to you that there are 19 countries that fall into UTC+3 --
MR. KOSTO: Objection, foundation.
THE COURT: Do you know one way or another?
THE WITNESS: I don't know.
THE COURT: Okay.
Q. UTC+2, are you familiar with that time zone?
A. Like, I understand that there is a time zone of -- because each one of them have a number, but I'm not sure what it represents.
Q. So UTC+2 is just an hour away from UTC+3?
A. Yes.
Q. UTC+4 is just an hour away from UTC+3 as well, correct?

A. Yes. That sounds right.
Q. UTC+2 is just, I guess, an hour behind UTC+3, correct?
A. Right.
Q. So UTC+2, do you know how many countries are within that time zone?
A. No.
Q. And Zulu time is what, based on your review?
A. In the context of this, it's the time stamp that was located within the data that I reviewed.
10:30 Q. Yes, but you converted Zulu into, for example, Pacific Central, correct?
A. Correct.
Q. So Zulu is which time zone on the UTC universe?
A. It represents, like, the starting point from which the other time zones --
THE COURT: Do you know what city?
THE WITNESS: Oh, it's in London.
Q. So it's in London. So London is about three hours behind Moscow, one hour behind Paris. It's fair to say it's two hours
10:30 behind Athens?
A. If that's where Athens is located, then, yes.
Q. So UTC --
THE COURT: She doesn't know, so I think you're going to have to do this in a different way.
Q. You also reviewed millions of line items and log files; is

that correct?
A. I didn't review millions. I know that they represent the universe from which the information was retrieved from.
Q. Did you do the retrieval? Did you yourself search for download.ASPX?
A. From the millions of lines of data, I did not pull it myself.
Q. Somebody else did that for you?
A. And then I validated it.
10:31 Q. Was it Mr. Kosto or Mr. Frank?
A. I don't believe it was either one of them.
Q. Mr. Kosto asked you to testify about Exhibit 176. It was a letter regarding certain IP addresses. Do you recall that?
A. Yes.
Q. Do you have any knowledge whether that IP address was actually on a Boston server?
A. I don't know.
Q. Could we pull up Exhibit 195I. This is one of the last charts that you testified about, correct?
10:31 A. Yes.
Q. And this is a chart that continues from February 5, 2018, to November 2, 2020, correct?
A. Yes.
Q. You didn't listen to the testimony in this case, correct?
A. I didn't listen to any of the testimony.

Q. And you didn't listen to the testimony of Mr. Hartvigson, who described the accounts that were affected by --

MR. KOSTO: Objection.

THE COURT: I haven't heard the question yet.

MR. KOSTO: He's stating another witness's testimony.

THE COURT: Overruled.

Do you know anything about that witness -- what's the question? You didn't hear any witness, so is there another way of framing the question?

10:32 Q. Mr. Frank and Mr. Kosto specifically asked you to include these five accounts, correct?

A. So these specific five accounts were included within the data that I received, which I then verified as to the universe.

Q. And you don't know whether the witness that was responsible for investigating the intrusions testified whether these five accounts were involved in the intrusion, do you?

A. I don't know anything about that.

MR. NEMTSEV: Nothing further.

THE COURT: Anything?

10:33 MR. KOSTO: Nothing.

THE COURT: Thank you. You may step down.

(Witness excused.)

MR. KOSTO: May I proceed, your Honor? Erik Uitto, U-i-t-t-o.

ERIK UITTO

having been first duly sworn, was examined and testified as follows:

THE CLERK: Please state your name, and please spell it for the Court Reporter.

THE WITNESS: My name is Eric Uitto, and it's spelled E-r-i-k. Last name is spelled U-i-t-t-o.

THE COURT: Now, make sure you speak nice and loudly so that your voice catches. Why don't you say your name again so you can hear your voice catch.

10:34

THE WITNESS: My name is Erik Uitto.

THE COURT: Okay.

MR. KOSTO: May I proceed?

THE COURT: Yes.

DIRECT EXAMINATION BY MR. KOSTO:

Q. Where do you work, Mr. Uitto?

A. I work for the Federal Bureau of Investigation.

Q. And what city do you work in?

A. I work in Huntsville, Alabama.

10:34

Q. What's your title at the FBI?

A. I am an IT specialist/forensic examiner.

Q. Are you a law enforcement agent?

A. I am not, no.

Q. And do you work within a particular division at the FBI?

A. Yes. I work within the Operational Technology Division.

Q. Is that sometimes referred to as OTD?
A. Yes.
Q. And what is OTD's task?
A. So we fight crime through technology.
THE COURT: You know, I can barely hear you. See, you can hear your voice catch if you move it close to your mouth. All right, so what's the division you're in again?
THE WITNESS: I'm in the Operational Technology Division.
10:35 THE COURT: Great.
Q. Use your halfway between inside and outside voice maybe.
A. Okay.
Q. And what does OTD do?
A. So we fight crime through technology.
Q. And within that -- that's a pretty broad statement -- what is your role in that process?
A. So I specifically work in the area of digital forensics.
Q. How far did you go in school?
A. I have a master's degree in computer science.
10:35 Q. And do you also have a bachelor's degree in information and computer science?
A. Yes.
Q. How long have you been an employee of the FBI?
A. It's about 14 years now.
Q. And you mentioned you're in digital forensics and your

title is forensic examiner. Can you tell the jury what it is a forensic examiner does.
A. So I support the agents. We go out and collect digital evidence. So we may go assist them during search warrants. We'll help seize servers, laptops, computers, telephones, those sorts of things. And then we'll bring them back to a laboratory environment, and there we'll analyze and process the devices and then write reports about them, and let the agents know what we find, and also we'll provide testimony in court like I am here.
Q. What is the CART team, C-A-R-T?
A. So CART stands for Computer Analysis Response Team, and it's the group within the FBI that's over all the digital forensic examiners like me.
Q. And so you're on the CART team?
A. Yes.
Q. Do you hold any certifications relevant to your work as a digital forensic analyst?
A. Yes.
Q. Can you name a few of them.
A. So I have certifications from the FBI, internal ones, ones that cover Windows forensics. There's one for Unix forensics, cellphone forensics, Macintosh or Mac forensics.
Q. You've named Windows, Unix, and Apple?
A. Yes.

Q. Are each of those different operating systems?
A. Yes.
Q. And they work in different ways?
A. Yes.
Q. So you get training on each of them?
A. Yes.
Q. Do you have any training in relation to malware?
A. I do, yes.
Q. And what is that?
10:37 A. So I have a certification, a GREM certification from an organization called SANS.
Q. SANS, S-A-N-S?
A. Yes. It's an outside organization. It's not government owned. It's privately run.
Q. And what does your training in malware from SANS mean you know about?
A. So there is a week-long training and certification that they offer, and it covers the topics of identifying malware and analyzing it and finding out how it works.
10:38 Q. And what is malware?
A. So malware is software that you don't want on your computer or device. It often takes actions without the consent of the owner or the user.
Q. I think you mentioned that your training from SANS involved reverse engineering malware; is that right?

A. Yes.
Q. And so what does it mean to reverse engineer malware?
A. That's looking at how it works, finding the details of it.
Q. Taking it apart, putting it back together?
A. Yes.
Q. In addition to your certifications, have you led trainings within the FBI on digital forensics?
A. Yes.
Q. Have you attended trainings inside and outside the FBI on
10:38 the same topic?
A. Yes.
Q. And have you testified in court concerning your work in computer forensics?
A. Yes.
Q. What kind of matters have you testified about?
A. In a computer intrusion case and then two human trafficking cases.
Q. And what kind of computers have you generally examined in connection with your work?
10:39 A. All three of those involved server computers. I have also examined laptops and desktops.
Q. Server, is that the physical box that contains the computer?
A. Yes.
Q. And what did you do for a living before you joined the

FBI?
A. I was a systems engineer working as a contractor for the Navy.
Q. And over the course of your time at the FBI, how many forensic exams would you say you performed on servers, laptops, phones, computers?
A. It's in the hundreds.
MR. KOSTO: Your Honor, the government would offer Mr. Uitto pursuant to Rule 702 in digital forensics.
10:39 THE COURT: All right. He can render an opinion.
Q. Now, in the course of your work, have you examined something called "virtual servers" or "virtual computers"?
A. Yes.
Q. Everybody in this room is looking for a good definition of virtual servers, so here's your chance.
A. Okay. So a virtual server is a physical machine that can run multiple operating systems. So you're probably familiar with Windows or Mac or Linux, these types of operating systems. You can have one physical machine that runs multiple operating
10:40 systems. It could have three Windows operating systems running on the one physical machine, plus two Linux ones.
Q. All in the same physical box?
A. Yes.
Q. All with the same power cord?
A. Yes.

Q. All with the same Internet connection?
A. Yes.
Q. And have you examined virtual servers over the course of your career in forensics?
A. Yes.
Q. And can you have as many virtual servers as you want in one physical box, one physical computer?
A. Usually there is a limit.
Q. What's the outer limit for how many you could have?
10:41 A. It's all the computer resources, so how much memory and processors you have.
Q. So the more powerful the physical computer, maybe the more virtual servers you can have in it?
A. Yes.
Q. And what is the advantage as an operator of running a virtual server, as opposed to having a physical computer?
A. So if you're running just one physical machine, it's often more efficient than running multiple independent ones, multiple physical machines.
10:41 Q. Why is that?
A. It saves on energy, it saves on cooling costs, these sorts of things.
Q. So if you have a datacenter, you can pay for one spot, not ten?
A. Yes.

Q. Do you need to be in any particular place as a user to access a virtual server?
A. Yeah, so servers usually don't sit in front of it when you're working with it. You can be anywhere in the world, really.
Q. And how is it that you access a virtual server if you're not next to it?
A. Virtual servers, you can often use a username and password to log in remotely.
10:42 Q. Let me direct you to the period of time beginning in or about July, 2020, and thereafter. Did you do digital forensics in connection with this investigation?
A. Yes.
Q. And who asked you to do that?
A. It was Special Agent David Hitchcock of the FBI.
Q. And what did he ask you to look at?
A. He asked me to look at a total of nine virtual servers.
Q. And do you know where they came from?
A. Yes.
10:42 Q. Where did they come from?
A. There were three that came from a virtual service provider called Digital Ocean, and there was six that came from a provider name Vultr. It's spelled V-u-l-t-r.
Q. And what are DigitalOcean and Vultr?
A. So they are both virtual server providers. They rent

servers over the Internet to users around the world.
Q. So if I had an account with DigitalOcean, I could sit down with a username and a log-in and get to a virtual server?
A. Yes.
Q. And was each of the nine computers that you looked at a virtual server?
A. Yes.
Q. And did Agent Hitchcock task you with any forensic responsibilities? What did he ask you to do?
10:43 A. So he wanted to know what or how the servers were configured and what they were doing. He also wanted to know information about the people running them, including potentially identifying them. He also wanted to know if there was any software known as Empire PowerShell.
Q. So if I have you right, three tasks: who was operating it?
A. Yes.
Q. And what was going on on the machine?
A. Yes.
10:44 Q. And whether there was Empire PowerShell on these machines?
A. Yes.
Q. Let me ask you first some questions about how these nine computers you looked at were set up. First of all, remind us one more time, how many?
A. There was nine servers in total.

Q. Six from what company?
A. Six from Vultr and three from DigitalOcean.
Q. And how did you keep track of each one? How did you distinguish among them?
A. So there was an IP address or Internet protocol address assigned to each.
Q. Each of the nine had their own IP address?
A. Yes.
Q. And did each of the nine also have a name that was
10:44 associated with it?
A. Yes. I identified that through my forensic exam.
Q. In preparation for your testimony today, did you work with my office to prepare a visual aid?
A. Yes.
Q. And would it assist you in explaining your forensic work to the jury?
A. It would.
MR. KOSTO: Your Honor, may I flip the physical version of this chalk around?
10:45 THE COURT: To whom?
MR. KOSTO: To the jury.
THE COURT: I haven't seen it yet.
MR. KOSTO: Ms. Lewis, would you please put it up on the screen. I don't think there's any objection to it.
THE COURT: You've all seen it?

MR. KOSTO: We showed it to Mr. Nemtsev, yes.
MR. NEMTSEV: Yes.
THE COURT: All right, so that's what I have on the screen? All right, thank you. There's no objection.
MR. KOSTO: Thank you, Mr. Frank. If you'd flip that around.
Q. Is what you have on your screen the same thing as what the jury has in physical form, as well as on their screens?
A. Yes.
10:45 Q. And we'll call it Exhibit DDD, if that's okay.
A. Okay.
Q. Do you recognize it?
A. I do.
Q. What is it?
A. So this is a digital depiction of the servers that I examined on the right there, so they each have a number on them, 1 through 9.
Q. Let me focus you first on the computers numbered 1 through 7. Do you see them there?
10:46 A. Yes.
Q. Are they kind of in a sideways V configuration?
A. Yes.
Q. Okay. And what do computers 1 through 7 show on this Exhibit DDD?
A. They functioned as gatekeepers for the furthest machine to

the right, server number 8.
Q. And when you say "gatekeeper," is there a technical term for that?
A. Yes. So the technical term is a "reverse proxy."
Q. Can you explain to the jury, in a easy for me to understand way, what a reverse proxy or gatekeeper is in this chart, 1 through 7.
A. Yes. So in this chart, it would function -- so the seven that are in that V formation, they would pass traffic to server
10:47 number 8, if it was coming from an infected machine; and if it was something else, it would send the traffic to some other website.
Q. Was there software that served this gatekeeping function on these virtual machines?
A. Yes.
Q. And what was it called?
A. The software is called NGINX. It's spelled N-G-I-N-X.
Q. And were computers 1 through 7 each running NGINX?
A. Yes.
10:47 Q. And which computer were the seven gatekeepers serving as a gatekeeper for?
A. For the server number 8 on the right, the Empire server.
Q. You call it the Empire server on the chart. Why do you call it that?
A. That is the server where I identified Empire PowerShell,

one of the three items that Agent Hitchcock asked me to look for.

Q. Based on your examination, and you can certainly refer to the chart, what were the names associated with computers 1 through 7?

A. So the first one was www.smartfinancelist.com. And server number 2, www.scoreyourmoney.com. Server number 3, www.developingcloud.info. Server number 4, cloudAPIfinance.info. Server number 5, www.finshopland.me. Server number 6, www.shopservice.live. And server number 7, www.Appfinreport.info.

Q. What's wrong with number 9 up there? Why is he off on his own?

A. So they had the same software NGINX running, but it was not configured as the other ones to function as a gatekeeper. It wasn't set up in the same way.

Q. And you have traffic lights next to each of 1 through 7; is that right?

A. Yes.

Q. What would happen, the way these computers were configured, if a network administrator typed in, say, "cloudapifinance.info" in their browser?

A. So it would send that network administrator to another website. It would prevent the traffic from going to server number 8, the Empire server.

Q. Let's look at how that might work.

MR. KOSTO: Ms. Lewis, would you please bring up Government's Exhibit 158.

Q. Do you recognize this?

A. Yes.

Q. And there's a lot going on there, but what is it?

A. It is a configuration file for the NGINX reverse proxy software.

Q. And this is a file related to the gatekeeper?

10:50 A. Yes.

MR. KOSTO: Okay, and I'd offer 158.

(Exhibit 158 received in evidence.)

MR. KOSTO: There's a lot of text going on there, but if you take us, Ms. Lewis, to just about that spot where it says "financecloudAPI.com."

Q. Do you see that there, Mr. Uitto?

A. Yes.

Q. Can you explain in laymen's terms what this file is showing about the Gatekeeper program.

10:50 A. So you'll see three pieces of text: Mozilla cloud, check news, and check date, sort of near the middle there.

Q. What does Mozilla cloud, check news, and check date have to do with any of this?

A. It's looking for information from the connecting client.

Q. So if the communication comes in to the Gatekeeper, is the

Gatekeeper looking for those specific words?
A. Yes.
Q. And if it sees those words, where does the communication get to go?
A. It will pass the traffic on to server number 8, the Empire server.
Q. And if the software doesn't see those words "Mozilla cloud, check news, and check date," what happens to the communication?
10:51 A. Down at the bottom there is references to a website. It would send it there, the finance.strands.com/products/strands-api-hub.
Q. So that's what happens if the magic words aren't there?
A. Yes. So if it's not an infected machine, then it would send it to this other website.
MR. KOSTO: And I ask you to bring up Exhibit 158A, and I'd offer it.
(Exhibit 158A received in evidence.)
Q. Can you read the top or the beginning of the domain.
10:52 A. It is strands.com.
Q. And what is this website in relation to the Gatekeeper?
A. It appears to be the third website that traffic would be sent to. So if it's not an infected machine, this is where it would be sent, the traffic.
Q. Is this what an administrator would see if they typed in

"cloudapifinance.info"?
A. Yes.
MR. KOSTO: So, Ms. Lewis, if you'd move Exhibit 158 to the right, and I'd ask you to bring up Exhibit 240 in evidence.
Q. And just as a reminder, on the left is the Gatekeeper, right? On the left is the Gatekeeper, correct?
A. Yes.
Q. And it's looking for "Mozilla cloud, check news, and check
10:52 date," right?
A. Yes.
Q. Could I have you take us -- first of all, could I have you read us the name of the machine in the bottom third of Exhibit 240, next to the word "computer."
A. So next to computer there, it says USD10846.TM.ToppanMerrill.com.
MR. KOSTO: Ms. Lewis, would you take us to Page 5 of Exhibit 240, the last dozen or so lines.
Q. In Exhibit 40, Mr. Uitto, do you see reference to the word
10:53 "Mozilla cloud"?
A. Yes. It's in the center there, a little towards the left, "Mozilla cloud," and then behind it is "Apple Web."
Q. Do you also see reference in Exhibit 240 to the words "check news" and "check date"?
A. Yes, the third line from the bottom.

Q. And do you see a reference to cloudAPIfinance.info?
A. Yes, over to the left.
Q. And is that the same domain that's in the Gatekeeper exhibit that we've been looking at?
A. Yes.
Q. So would a communication that had this code in it from Exhibit 240, would that get to the Empire server, or would it get rejected and sent to the website?
A. It would get to the Empire server, so it would be passed through.
Q. Why?
A. Because it contains that text that it was looking for, so specifically "Mozilla cloud" and "check news."
Q. And if an administrator was trying to figure out what cloudAPIfinance.com was and they didn't have "check news, check date," or "Mozilla cloud," would they be able to?
A. No.
Q. Practically speaking, what function was the Gatekeeper computer serving here?
A. It would, yeah, only prevent infected machines giving them access to server 8 and blocking all the rest.
Q. And you said earlier that server number 8 was called the Empire server?
A. Yes.
Q. Because it had Empire PowerShell on it?

A. Yes.
Q. What is Empire PowerShell?
A. So it's software that can be used to remotely control a machine.
Q. Let's discuss some things that you found. Did you look in the PowerShell server, the Empire server, number 8?
A. Yes.
Q. Let's discuss some things you found there. I'm showing you and offering Exhibit 159 --
10:55 MR. KOSTO: Unless the Court would like to stop now and give everyone a break.
THE COURT: How much more do you have with this witness?
MR. KOSTO: More than five minutes and less than 20.
THE COURT: Till 11:00, and then we'll take our break.
Q. I'm showing you Government Exhibit 159. Do you recognize it?
A. Yes.
Q. What is it?
10:55 A. So this is an agent log file regarding one of the infected machines.
Q. And can you read the name of the infected machine under the word "username."
A. The host name?
Q. Yes.

A. "USD10846."
Q. And where did you find this log file, agent.log file?
A. This was on server number 8, the sort of first on the right on the chart.
Q. The one behind the Gatekeepers?
A. Yes.
Q. And what is an agent.log file?
A. So it contains information from one of the infected machines.
10:56 THE COURT: "Infected" means what, again?
THE WITNESS: That there is unwanted software running on the machine.
Q. Where in this case were the infected machines from?
A. So in the log, agent.log, there is the reference to the domain Toppanmerrill.com, as well as that host name for the full USD10846.TM.Toppanmerill.com.
Q. So it's fair to say the log is reflecting communications from Toppan Merrill?
A. Yes.
10:57 Q. But this isn't a Toppan Merrill log, is it?
A. It's not. This is from server number 8, the Empire PowerShell server.
Q. Okay. And why would the Empire PowerShell server have communications from a Toppan Merrill computer in it?
A. Since it was controlled through this Empire PowerShell.

THE COURT: So was that Toppan Merrill's?

THE WITNESS: So I did not examine Toppan Merrill's systems but --

THE COURT: Whose server was it, this Empire shell?

THE WITNESS: So server number 8 on the right, so the chart --

THE COURT: Yes, but who's was it? Do you know?

Q. What company hosted the servers numbers 1 through 8, or 1 through 9?

10:57 A. It was either -- either DigitalOcean or Vultr.

Q. So these were computers that were rented at DigitalOcean and Vultr that you examined?

A. Yes.

Q. And these were servers that were obtained by the FBI during the course of its investigation?

A. Yes.

Q. And do they have domain names that were related to the investigation in some way?

A. Yes.

10:58 Q. So that's why you were looking at these particular computers?

A. Yes.

Q. Okay. Now, on Exhibit 159, is there a date?

A. There is.

Q. What's the date?

A. December 23, 2019.
Q. And does this log tell you what kind of activity was going on on that Toppan Merrill computer?
A. Yes.
Q. What is the name of the software program that was running, according to this log, on Toppan Merrill's network?
A. Yeah, so the process name there was RDTEVC.
MR. KOSTO: Okay, Ms. Lewis, would you put 159 on the left and bring up Government's Exhibit 240, Page 1, in
10:58 evidence. And make that just a tiny bit bigger.
Q. 240 is from where, Mr. Uitto?
A. So this one on the right?
Q. Yeah. What company's logs are those?
A. It appears to be from Toppanmerrill.com.
Q. And what's the machine name?
A. USD10846.TM.Toppanmerrill.com.
Q. And does Exhibit 240 tell you the name of the software program that was running on Toppan Merrill's network?
A. Yes. There's a line for "host application," and at the
10:59 very end, it contains RDTEVC.exe.
Q. And so how does the RDTEVC on the right in Exhibit 240 relate to the RDTEVC on the left in Exhibit 159?
A. So that's the infected process that sent -- that created the logs on the left on the PowerShell server.
Q. The same program running in 240 on the right and reflected

in the logs on server number 8 on the left?
A. Yes.
MR. KOSTO: Is this a good time, your Honor?
THE COURT: This is a good time. It would be great to see you at sidebar for a minute.
(Jury excused.)
THE COURT: You can step down, sir. I'm sorry. I'm sorry.
SIDEBAR CONFERENCE:
11:01 THE COURT: How much longer with him?
MR. KOSTO: Fifteen minutes.
MR. NEMTSEV: Ten?
THE COURT: This is incomprehensible to me. I have no idea what you're talking about, and if that's true for me, perhaps it's true for the jury. I don't understand -- is there a way of sort of --
MR. KOSTO: I'm happy to --
THE COURT: Are you going to sum up at the end, in terms of why this all matters?
11:01 MR. KOSTO: Of course, your Honor.
THE COURT: How does it matter here? I was worried that --
MR. KOSTO: These are the six computers that were rented at DigitalOcean and Vultr that the victim companies were communicating with, that Toppan Merrill provided to the FBI,

right? The FBI went to Namecheap and found this domain.
THE COURT: Are they bad computers? Are they --
MR. FRANK: These are the hackers' computers.
MR. KOSTO: These are the hackers' computers.
THE COURT: That's not clear. From the get-go, that's not clear. And does that track back somehow -- you know, there's all these lines of code. Does it track back to M-13?
MR. FRANK: We already presented the evidence that it tracked back. These are the domain names that they found at
11:02 Toppan Merrill.
THE COURT: Right.
MR. FRANK: The domain names came back to Namecheap. Namecheap came back to DigitalOcean and Vultr, and that's what we went through with Agent Hitchcock.
THE COURT: Yes.
MR. FRANK: So all those IP addresses traced back, and now we're looking at the actual computers from DigitalOcean and Vultr. So those domain names were placed on those rented computer servers.
11:02 THE COURT: Yes?
MR. FRANK: That's these eight computers.
THE COURT: Can't you just say that in seven questions?
MR. FRANK: Sure, we will clear that up, and then what he --
THE COURT: We're looking at all this code. It's A --

MR. FERNICH: He's just trying to read the report.

THE COURT: Let me just say this: A, it's deadening, and, B, it's incomprehensible.

MR. FRANK: Judge, it's meeting our burden. We --

THE COURT: Excuse me. You've got to only meet a burden by making it understandable.

MR. FRANK: The reason it's relevant is because the malware that was found on the Toppan Merrill system, which Mr. Kosto will establish that the way that the hackers controlled the Toppan Merrill computers and got it to export the confidential information, that same malware was found on these servers, which we've tied to M-13.

11:03

MR. KOSTO: Mr. Brawner testified about --

THE COURT: Excuse me, excuse me. Let me just say this: I'm not doubting that it's relevant. I'm just saying it's not comprehensible about where we are going. We're looking through -- for me anyway, who never took computer science, and my bet is none of these except maybe one guy, has no idea why they're looking at all this.

11:03

MR. KOSTO: We'll clear it up, your Honor.

THE COURT: All right. So then who's the next witness?

MR. KOSTO: Mr. Kenney, Bitcoin.

THE COURT: Is he going to be clearer?

MR. KOSTO: Yes, I think -- well, we have a different

opinion about the clarity, but Mr. Kenney will testify about the Bitcoin analysis that he performed.

MR. FERNICH: It's going to be worse.

THE COURT: Is it going to be worse?

MR. KOSTO: Respectfully, I don't think that Mr. Fernich has met the witness or talked to him.

THE COURT: I'm not saying this guy isn't relevant. I'm just saying it's hard to figure out where this is going.

MR. FRANK: The reality is, the burden that we have is, these are sophisticated hackers using very sophisticated techniques.

11:04

THE COURT: Let me just say this: That may be. It's got to be understandable.

MR. KOSTO: I understand.

THE COURT: Now, the next thing is, so the Bitcoin guy takes how long?

MR. KOSTO: Thirty-five minutes on direct.

THE COURT: Okay, in plain English.

MR. KOSTO: Yes.

11:04

THE COURT: And then how long on cross?

MR. NEMTSEV: Ten?

THE COURT: And then who?

MR. FRANK: It looks like we'll probably get to Mr. Clarke, to start Mr. Clarke today.

MR. NEMTSEV: We haven't discussed Mr. Clarke. We

have objections to some of the exhibits that he wants to put in and --

THE COURT: Well, we'll see how far we get. But let me just say this: What I'd like you to work on Clarke is the way we talk about "trillion." So a limiting instruction, if someone drafts it for me, I'd be happy to do it.

MR. FRANK: We'll draft it.

THE COURT: That was the big issue, as I remember, coming out of it.

11:05 MR. FERNICH: On the last two columns of the chart.

THE COURT: I haven't seen the chart.

MR. FERNICH: He testified --

(Cross-talk.)

THE COURT: I don't remember them, so that --

MR. FERNICH: That's what incorporates what they're calling the p-value, which is a different way of expressing the ratio of one in a trillion, or whatever it was.

THE COURT: So we won't put that up until after I've resolved that question.

11:05 Okay. Now, one last question is with the woman who did the summary charts from the office?

MR. KOSTO: Ms. Yanochko.

THE COURT: Some of those IP addresses you emphasized in the beginning of your discussion with the agent yesterday.

MR. KOSTO: Yes.

THE COURT: They were familiar to me, and I remembered them, but a bunch of the IP addresses I didn't recognize.

MR. KOSTO: Yes.

THE COURT: But they may not realize that we haven't discussed them, so I want to be clear to them.

MR. FRANK: Your Honor, it's all -- they used many IP addresses as part of the conspiracy.

THE COURT: What?

MR. FRANK: 110. We're not going to trace each and every one back.

11:06

THE COURT: Excuse me, excuse me. That may be, but no one, except maybe you all, have memorized all of them. And so you very nicely yesterday tied back 189 and 119, or something like that, and the 104, so we've got three, but a bunch of them I don't remember having discussed before.

MR. KOSTO: And what we might suggest is that it's not so important which IP address they came from but what was happening with that IP address: the same downloads, the same user, the same companies, the same kind of information, all of which ties it to the actors.

11:06

THE COURT: Was there trading by these --

MR. FRANK: Yes.

THE COURT: That's the key.

MR. FRANK: We haven't gotten there yet.

MR. KOSTO: It's coming.

THE COURT: But you'll tie that in, those downloads, even though we don't recognize the IP address?

MR. FRANK: That's correct.

MR. KOSTO: There's a lot of different kinds of evidence that has --

(Cross-talk.)

THE COURT: Good luck to you. Good luck to you. You're going to have some experts who are going to sort of try and explain it?

11:07 MR. NEMTSEV: Yeah. I'm trying to figure out -- your Honor told them Thursday, but I don't think it's going to be Thursday. Wednesday?

MR. FRANK: If we start Mr. Clarke today, then your experts, unless you have some massively long cross of Mr. Clarke, will be in tomorrow.

THE COURT: So you might want to have them here.

MR. NEMTSEV: I don't know if I can get both of them here, though.

THE COURT: One anyway. And am I going to be getting

11:07 anything on the jury instructions?

MR. KOSTO: Yes, your Honor, three or four pages with some minor suggestions.

THE COURT: That's fine. Just, you know, if there's anything we need to look up. We've been doing a lot of research on venue, I have to say, which turns out to be an

interesting issue. The Second Circuit requires a jury to try it on venue if there are disputed facts, which there are here. The Ninth Circuit suggested special interrogatories, which none of you seem to want.

MR. NEMTSEV: We don't want that.

THE COURT: You've said "no" too, so you're both on the same page. If you agree, which is rare, I agree.

And then, as far as I'm concerned, while there is some leeway for a judge if it's undisputed facts, I think there are disputed facts here, so it will go to the jury.

11:08

MR. FERNICH: And I'd like to be heard on that at Rule 29 time, either orally or in writing. I'm not sure -- I'm working it in my head right now -- what I want to do with that.

THE COURT: Maybe. I understand you have a real -- I don't even know if Rule 29 applies here, but if it does, let me just say this: I'm not dealing with that issue. I'm dealing with the issue of -- it turns out Judge Woodlock wrote a very nice opinion saying it was unsettled in the First Circuit, as usual, but basically most circuits I think are trying venue when there are disputed facts.

11:08

MR. FERNICH: Yes. And I think that even taking the facts in the light most favorable to the government, they haven't established venue as a matter of law.

THE COURT: Then it will be going to the jury.

MR. FERNICH: Okay.

THE COURT: Okay? I haven't heard the whole case yet, but at least --

MR. FERNICH: I understand, I understand.

THE COURT: I don't want to spend the time. We all need a break.

(End of sidebar conference.)

(A recess was taken, 11:09 a.m.)

(Resumed at 11:38 a.m.)

THE CLERK: All rise.

11:37 (The Court entered the courtroom.)

MR. FRANK: Your Honor, we have a proposed instruction for Mr. Clarke.

THE COURT: Mr. Clarke?

MR. FRANK: For his testimony.

THE COURT: Okay.

(Handed up instruction.)

Did you share it?

MR. NEMTSEV: Now they did.

(Pause.)

11:38 THE COURT: Okay. So you guys can play with it, if you want something else.

Can I also say that I need a copy of this chalk for the record, if we have one printed out.

MR. KOSTO: We'll print one for you, your Honor.

THE COURT: Yeah, I think we need to keep that in the

record.

Could you just move it a little bit, because it blocks two of the jurors, so I can't see them.

MR. KOSTO: Sure.

(Pause.)

THE COURT: Where is the witness?

MR. KOSTO: We'll bring him in.

THE CLERK: All rise for the jury.

(Jury entered the courtroom.)

11:40 THE COURT: Okay. Power on until 1:00. Let's go.

Sir, you may sit down, and you're still under oath.

I'm speaking only for myself, but as someone who's not a computer scientist, if you could just sort of speak in plain language so we can really follow this, it would be helpful.

They're all laughing. They must all have PhDs in computer science, I'm sure. But it's a little hard to follow, so maybe take baby steps.

All right, go ahead.

MR. KOSTO: In that vein, may I continue, your Honor?

11:40 THE COURT: Yes.

BY MR. KOSTO:

Q. Let's go back about a hundred feet, Mr. Uitto.

First of all, in your illustration, your chart, computers 1 through 9, are those the ones on the right-hand side of your chart?

A. Yes.
Q. Computers 1 through 7 were that gatekeeper, right?
A. Yes.
Q. Okay. And computer 8 is the one we've been calling the Empire server, right?
A. Yes.
Q. That's the one with PowerShell on it.
A. That's correct.
Q. And just remind us where computers 1 through 8 came from. Where were they in the internet?
11:41
A. They came from the two providers, DigitalOcean and Vultr.
Q. And that's even actually written down in the left-hand corner of your illustration, right?
A. Yes.
Q. We've got computers number 1 and 2 came from DigitalOcean, right?
A. Yes.
Q. And computers numbers 3 through 7 and 9 came from Vultr?
A. Correct.
11:41
Q. And these were the servers that you examined?
A. Yes.
THE COURT: And they're not Toppan Merrill servers, right?
THE WITNESS: That's correct.
THE COURT: When you called them "infected," what did

you mean by infected?

THE WITNESS: So there's logs contained from Toppan Merrill servers, logged information --

THE COURT: Is it the hacker's servers?

MR. KOSTO: I think I can clear this up, your Honor.

THE COURT: Okay, go ahead.

BY MR. KOSTO:

Q. So 1 through 8 are what you looked at?

A. Yes.

11:42 Q. And there was malware on those computers, right?

A. Yes, I would call it malware.

Q. And those were the ones from DigitalOcean and Vultr?

A. Yes.

Q. Those are the hacker's computers, right?

A. Yes.

Q. The computer on the left in your chart is Toppan Merrill, right?

A. Yes, the Toppan Merrill network or computers, yes.

Q. Toppan Merrill is the alleged victim in this case, right?

11:42 A. Yes.

Q. And your chart is designed to show communications between the victim computers and the hacker computers, right?

A. Yes.

Q. And what happened to those communications when they got to the hacker computers?

A. They were stored, some of them, or the logs were stored there.
Q. And you found them when you did your forensic analysis on the hacker computers?
A. Yes.
Q. And what we're looking at now with these exhibits is what you found on the hacker computers, right?
A. Yes.
Q. And occasionally, we're going to put up an exhibit that comes from the victim's computers, yes?
A. Yes.
Q. And we're going to compare what was on the victim's computers with what was found on the hacker's computers; is that right?
A. That's correct.
Q. All right. Let's try it once and see how it goes.
THE COURT: So is 8 a hacker computer?
THE WITNESS: Yes.
BY MR. KOSTO:
Q. And is number 8 the computer that you've been calling the Empire server?
A. Yes.
Q. And why did you call it that?
A. That's where the Empire PowerShell software was running.
Q. And PowerShell was one of the things that Special Agent

Hitchcock asked to you look for, right?
A. Yes.
Q. Because it was also found on the victim's computer.
A. That's correct.
THE COURT: And what's PowerShell?
THE WITNESS: Empire PowerShell, I would call it malware.
THE COURT: All right. So that's what you're calling the malware?
11:43 THE WITNESS: Yeah. Microsoft, they have software known as Windows Defender that runs by default on the Windows operating system, and they classify Empire PowerShell agents as malware.
THE COURT: So the malware is on 8?
THE WITNESS: It controls the malware that's on --
BY MR. KOSTO:
Q. Excuse me, Mr. Uitto, is the malware also on the victim's computers?
A. Yes.
11:44 Q. And in the examples we're going to be going over here today, is it the same malware that's on the victim's computers and the hacker's computers?
A. It's the agent or the client, while 8 is the server that controls --
Q. Let's take a look at one of them and see what happens,

okay?
A. Okay.
Q. Let's bring back up Exhibit 159.
You testified before break that this was an agent.log file.
A. Yes.
Q. Let's start with the simple question of what computer did you find this file on? Forget what's in it, just where did it come from?
11:44 A. This came from the server furthest on the right, the server number 8 or the Empire server.
Q. Okay. So the hacker computer?
A. Yes.
Q. Okay. And you found this file in the hacker computer?
A. Yes.
Q. And this file, number -- this file is -- it's got a computer name associated with it, a host name.
A. That's correct.
Q. Can you read that aloud?
11:45 A. So it is USD10846.
Q. Even though that says "USD," where did you find this?
A. On server number 8.
Q. Not on a Toppan Merrill computer, on the hacker computer?
A. That's correct.
Q. And what does the fact that there's a computer named -- a

log of a computer named 10846 on the hacker computer tell you?
A. It tells me that this machine was infected -- this machine that I did not examine, but there are log files from it.
Q. So there's a Toppan Merrill machine that's communicating with the hacker machine, and that machine is named USD10846, right?
A. Yes.
Q. Okay. What's the date that this infected computer at Toppan Merrill communicated with the hacker computer number 8?
11:45 A. December 23rd, 2019.
Q. And is there something on this log that you found that tells you the name of the program that was running on the victim's computer at Toppan Merrill?
A. Yes, the process name line, and that reads rdtevc.
Q. And is process another name for computer program?
A. Yes.
Q. So this is a log that shows that a program named RDTEVC was running on a Toppan Merrill computer, right?
A. Yes.
11:46 Q. But it's stored in the hacker computer?
A. That's right.
Q. The log is stored there, but it's a record of what's going on at Toppan Merrill?
A. Yes.
Q. Okay.

THE COURT: Is that the malware?
THE WITNESS: rd --
BY MR. KOSTO:
Q. What is RDTEVC?
A. So that is the Empire PowerShell agent, one of them. So, yes, that would be -- if you ran it, Windows Defender, it would classify that as malware. So Microsoft would call Empire PowerShell agent's malware.
Q. And what does PowerShell do? You can call it anything, right? You can call it RDTEVC?
11:47
A. That's probably a randomly chosen name.
Q. But no matter what it's called, what does it do?
A. So it allows it to be remotely controlled and accessed.
Q. Allows what to be remotely controlled and accessed?
A. The infected machine.
THE COURT: That means you're the hacker machine? When you say "infected machine," are you referring to the hacker machine or the victim machine?
THE WITNESS: Victim machine.
11:47
THE COURT: So when you say "infected" -- you've been using that term a lot -- sometimes it's the hacker and sometimes it's the victim?
THE WITNESS: I think the two terms we've used are "malware" and "infected," and we've used --
BY MR. KOSTO:

Q. Let's just -- if we can, Mr. Uitto, let's use "hacking computer" and "victim computer."
A. Okay.
Q. When you refer to infected machines, are you referring to the hacking computer or the victim computer?
A. Victim.
THE COURT: So 1 through 7 are what?
THE WITNESS: Those are all hacker machines.
THE COURT: Those are all hacker, not infected?
11:48 THE WITNESS: That's right.
BY MR. KOSTO:
Q. And how about number 8?
A. That's also a hacker machine.
Q. And the infected computer on your chart is where?
A. On the very far left.
Q. The one that says "Toppan Merrill" underneath it?
A. Yes.
Q. Now, you've talked about this program, PowerShell, running on the infected machine, the machine at Toppan Merrill.
11:48 A. Yes.
Q. And what was the name of the program that was running on the machine at Toppan Merrill, the victim's computer?
A. It was that RDTEVC.
Q. Okay. And what date was it running on?
A. December 23, 2019.

Q. Can we now see Exhibit 240 on the left.

Mr. Uitto, is it fair to say that Exhibit 240 comes from the victim machine?

A. Yes.

Q. The one at Toppan Merrill?

A. That's correct.

Q. And you know that how?

A. So there's a line down at the bottom, computer, and it has --

11:49 Q. What is the domain there?

A. It was toppanmerrill.com.

Q. So that tells you this is a log from the victim computer?

A. Yes.

Q. And does the log from the victim computer on the left tell you the name of the program that was running on this computer?

A. Yes.

Q. Can you read it aloud?

A. So at the very end of that long line there, it's rdtevc.exe.

11:49 Q. And so when you examine forensically this computer out there at DigitalOcean and Vultr, and you see RDTEVC on the hacker's computer and you see RDTEVC on the victim's computer, what does it tell you about the relationship between the hacker's computer and the victim computer?

A. That they were communicating and that that's where it

communicated through.
Q. They were communicating with each other?
A. Yes.
Q. And what program were they using to communicate with each other?
A. The Empire PowerShell.
Q. And is the same date on the hacker's computer and the victim computer?
A. Yes.
11:50 Q. And let me ask you one more question about the log from the hacker's computer.
About midway down the page, do you see an IP address labeled "External IP"?
A. Yes.
Q. This is in Exhibit 159, the hacker's computer.
Can you read that aloud?
A. Yes, the IP address is 45.77.65.69.
Q. Okay. Let's pause for a second.
Do you recognize that IP address?
11:50 A. I do.
Q. Is it a hacker computer or a victim computer?
A. It's a hacker computer.
Q. And is it one of the hacker computers that is on your chart?
A. Yes.

Q. Which one?
A. It's -- so the V-shaped formation, it's the very one at the tip, server number 4, I believe it is.
Q. So 45.77.65.69 was computer number 4?
A. Yes.
Q. And I'm going to direct your attention to page 48. We're going to skip way far down in Exhibit 159. Baby steps, though.
A lot of code here. We're not going to focus on all of it, Special Agent Uitto. Two full paragraphs from the
11:51 bottom --
MR. KOSTO: You can take down the one on the left, Ms. Lewis. Thank you.
Q. Two full paragraphs from the bottom, with the date 12/25/19 at 10:51:24, do you see that?
A. Yes.
Q. Just a reminder, which computers -- where did you find this log?
A. This was on server number 8, or the Empire server.
THE COURT: The hacker.
11:52 Q. The hacker computer?
A. Yes, the hacker.
Q. One of the hacker computers?
A. That's correct.
Q. And do you see the name of the program that's running on the hacker computer?

A. I do.
Q. And what is the name there?
A. It is migrate.exe.
Q. And what is migrate.exe?
A. So from other information I found on another system, it is actually different software known as PuTTY.
Q. Okay. Is something --
THE COURT: It's different software, what?
THE WITNESS: Known as PuTTY.
11:52 BY MR. KOSTO:
Q. And what does PuTTY do ordinarily, just in very, very basic terms?
A. So it's a way of making a secure connection between two computers.
Q. And when something is renamed, in your opinion, why is it renamed from what it's called PuTTY to something called migrate.exe?
A. To hide what it is.
Q. Can you go out and buy migrate.exe?
11:53 A. It's a free software, so PuTTY is free.
Q. But you'd have to rename it to migrate?
A. Yes.
Q. What does the renaming tell you about the use of that software?
A. So that it -- they're trying to hide it.

Q. And the "they" in this case who is trying to hide it is who? Not by name.
A. The attackers.
Q. The attackers, the hackers?
A. Yes.
Q. At the bottom of this line of the paragraph Ms. Lewis has highlighted, do you see the name tjerome?
A. Yes.
Q. Does that name mean anything to you as you sit here today?
11:53 A. That is the username that was used to log into server number 4.
Q. Let's pause there for a sec.
So what computer logged into server number 4?
A. So that was the USD10846, the Toppan Merrill, the infected machine.
Q. So a victim machine logged into computer number 4 in the diagram?
A. Yes.
Q. And what username did it use?
11:53 A. tjerome.
Q. And when did that take place, that login from the victim computer to the hacker computers?
A. It was on December 25th of 2019.
Q. Now, just a few more questions about this exhibit from the hacking computer.

Do you see on page 49 at 1:14 in the afternoon --

MR. KOSTO: If you'll highlight that section, please, Ms. Lewis.

Q. First of all, do you see tm.toppanmerrill.com?

A. Yes.

Q. What does that tell you is going on in this line of code?

Where did you find this code? We're still in the agent log, right?

A. Yes, so this was on server number 8.

11:54 Q. This is from the hacker computers, right?

A. Hacker computer, yes.

Q. And what is going on in this line of code? Put it in the plainest of English.

A. So the infected machine is being --

Q. The victim machine?

A. The victim machine is using -- or being used to check if another machine is online.

Q. What's the number for the other machine that the victim machine is looking for?

11:55 A. USD11150.tm.toppanmerrill.com.

Q. So this is one victim machine reaching out to talk to another victim machine?

A. Yes.

Q. But where was this little snippet of code found? Was it found on the victim machines?

A. No.
Q. Where was it found?
A. It was found on server number 8, the Empire server.
Q. The hacker --
A. The hacker machine.
Q. Okay. Now, one last question here.
At 1:15 on the next page, 1:15 p.m. --
MR. KOSTO: 13:15:00 on Christmas Day, Ms. Lewis, do you have it there? Thank you.
11:55 Q. -- I'm not going to get deep into this, but do you see the words "netsh"?
A. Yes.
Q. And what is netsh doing?
A. This command is opening a connection between two machines.
Q. Okay. Which two machines are communicating with each other?
A. So both of them are victim machines.
Q. And can we tell what the victim machines are saying to one another?
11:56 A. No.
Q. Why is that?
A. The connections would be encrypted.
Q. And so how does that help or hurt the attack to have the communications encrypted?
A. It would be difficult for those that are looking for

attacks to know what's going on.
Q. Like a system administrator.
A. Yes.
Q. All right. Let's go to a different one and hopefully an easier one. Thanks for your patience, Mr. Uitto.
MR. KOSTO: Can we please have 160, Ms. Lewis, and I'd offer it.
(Exhibit 160 received into evidence.)
Q. Do you have it in front of you, Mr. Uitto?
11:56 A. Yes.
Q. Is this another agent.log file?
A. Yes, it is. So it's from another victim machine.
Q. Okay. And which computer did you find this log file on, the hacker computers or the victim computers?
A. Victim computer. Or this was on the -- the hacker computer I found this log.
Q. Okay. And does the information in this log tell you anything about the victim computer?
A. Yes, there was a host name and a username.
11:57 Q. What was the username for the victim computer?
A. It's -- there's a username line there, and it's rbehm.
Q. And what was the name of this machine that was being recorded here?
A. That's the host name line, and that is USL10986.
Q. Okay. And does this log show a connection between a

victim machine and a hacking machine?
A. Yes.
Q. Which of the hacking machines does it show a connection to?
A. The line labeled "External_IP," the IP there is 45.77.33.100.
Q. And is that an IP address -- you don't have to memorize it, but is that an IP address that's already on your chart?
A. Yes, I believe it's near the bottom.
11:58 Q. Which computer number is that one?
A. I don't see the chart. I'd have to --
MR. KOSTO: I think Ms. Lewis could bring it up for you.
A. I think it's the bottom one.
Q. Do you see computer number 7 at the bottom?
A. Yes.
MR. KOSTO: Ms. Lewis, could you highlight the IP address.
Q. So Ms. Lewis has just highlighted computer number 7's
11:58 unique IP address, correct?
A. Yes.
Q. And what's the IP address?
A. It's 45.77.33.100.
Q. Is that the same IP address that the victim computer was communicating to?

A. Yes.
Q. And what was the date of that communication?
A. January 17th of 2019.
Q. All right. Were you able to identify by name the administrators of the hacking computers?
A. No.
Q. Why not?
A. They were sophisticated. They took steps to hide who they were.
11:59 MR. NEMTSEV: I object, your Honor.
THE COURT: Overruled.
What steps, could you tell?
BY MR. KOSTO:
Q. You said sophisticated. Why do you say sophisticated?
A. This setup that we see in the diagram where server number 8 is kind of hidden, or attempted to be hidden, that's a very sophisticated setup.
Q. How about the use of PowerShell in this way?
A. Yes, this was -- that's a -- not a simple tool to use.
11:59 It's one that takes some knowledge and know-how how to use that hacking tool.
Q. What does the use of this hacking tool tell you about what the hackers understood about computing?
A. They had an intimate knowledge of --
MR. NEMTSEV: Objection, your Honor.

THE COURT: Sustained.
BY MR. KOSTO:
Q. What about the use of the reverse proxy, what does that tell you about these hackers, if not their names?
A. That they were sophisticated.
Q. One last exhibit for you, Mr. Uitto. It's Government Exhibit 161. It's a 583-page document, but we're going to look at just one page, okay?
THE COURT: You're not introducing the whole thing, are you?
12:00
MR. KOSTO: No, we're offering it and we're going to refer to page 1. It will never be printed out, your Honor.
We'd offer 161.
(Exhibit 161 received into evidence.)
BY MR. KOSTO:
Q. And I'd ask you if you recognize Exhibit 161.
A. Yes.
Q. What is it?
A. So this is a script called Invoke-Mimikatz.
12:00
Q. Before you talk about Invoke-Mimikatz, could you tell us which computer it was found on?
A. This was found on server number 8, the Empire server, the hacker -- one of their machines.
Q. One of the hacker computers, okay.
What is Mimikatz?

A. So Mimikatz, it is software that can be used to steal credentials, which are usernames and passwords.
Q. And so Mimikatz was found where?
A. The software was found on server number 8.
MR. KOSTO: Let me ask you, Ms. Lewis, to pull up Exhibit 239 on the left from Toppan Merrill. Or the right. Either/or is fine.
Q. Can you read the date for this log from Toppan Merrill?
A. So the log line there is January 10, 2019.
12:01 MR. KOSTO: And, Ms. Lewis --
Q. Or could I have you read the name of the program that's referenced in the log file from the victim computer?
A. So there's a second line from the top in the center there, function Invoke-Mimikatz.
Q. What is the relationship between the Mimikatz on the victim computer and the Mimikatz on the hacking computer?
A. They both appear to match.
Q. Can I have you read the second sentence of the paragraph immediately below "Synopsis."
12:02 A. So in the right-hand one or the left one?
Q. Both, in the right-hand one.
A. Okay. So this script leverages Mimikatz 2.0 and Invoke-Reflective PE injection to reflectively --
Q. I'm going to have you skip to the second sentence, the one in English.

A. Okay.
Q. Beginning with "This allows."
A. "This allows you to do things such as dump credentials without ever writing the Mimikatz binary to disk."
Q. And looking at Exhibit 161 from the hacker computer, do you see the same sentence there?
A. Yes.
Q. Is this the exact same program on the hacking computer and the victim's computer?
12:02 A. Yes.
MR. KOSTO: Nothing further.
MR. NEMTSEV: Can we leave that up?
I'm sorry.
Your Honor, could I put next to Mr. Uitto his --
THE COURT: I can't hear a word you're saying.
MR. NEMTSEV: Can I put next to Mr. Uitto his expert report in case he needs to refer to it so I don't have to run back and forth?
THE COURT: If it's his expert report, that's fine
12:03 with me.
MR. NEMTSEV: It is. Thank you, your Honor.

CROSS-EXAMINATION

BY MR. NEMTSEV:
Q. Good afternoon, Mr. Uitto. My name is Max MR. NEMTSEV. You and I have never met before, correct?

A. That's right.
Q. And you just testified regarding the similarities and potentially the differences between these two programs that were located, one on the Toppan Merrill server, the other one on what you called was a hacker server, correct?
A. Yes.
Q. Do you see differences in terms of versions that were installed -- I lost it.
I got it back.
12:04 THE COURT: Is the mic not working?
MR. NEMTSEV: No, no, the screen stopped working.
THE COURT: Oh.
BY MR. NEMTSEV:
Q. Do you see the different versions between Exhibit 161 and the other exhibit that's on the screen on the right?
A. So I examined the one on the left. The one on the right, I believe, came from evidence.
Q. But you would agree that they're different versions?
THE COURT: Are you talking about different versions
12:04 of Mimikatz?
MR. NEMTSEV: Yes.
A. There is a different version line, Mimikatz Version 2.1, and then there's -- on the left it's 2016 11/26, and on the right it is 2018 06/16.
Q. And you would agree that the 2018 and the 2016, that

refers to the year that it was produced?
A. That's likely the case.
Q. And Mimikatz, to your knowledge, is a public, open-source program that anyone can download, correct?
A. Yes.
Q. And I believe in your report you referenced a link where I could go right now, open it up on my computer, click the "download" button, and I would be in possession of Mimikatz, correct?
12:05 A. Yes.
Q. And Mimikatz is -- Joe Bialek seems to be the author of Mimikatz, correct?
A. That's correct.
Q. Could this -- these are different versions, clearly, correct?
A. I'd have to see the complete file to see all of the differences, but there is a different version number in there.
Q. So it's unlikely that the version on the left made it onto the computers -- to the Toppan computers on the right?
12:06 A. I did not examine the computers on the right, so the Toppan Merrill computers. I only examined the virtual servers, so I --
THE COURT: You only looked at the so-called hacker computers?
THE WITNESS: That's correct.

THE COURT: You didn't look at Toppan Merrill's?
THE WITNESS: That's correct.
BY MR. NEMTSEV:
Q. And you looked at it to identify connections, correct, between the two computers?
A. There was logs that detailed connections between the two.
Q. Did those logs show you what files were downloaded, when they were downloaded?
A. In some cases, yes.
12:06 Q. Did they show you when and at what time, for example, earnings reports were downloaded?
A. I did not come across that during my examination.
Q. Did you see any evidence that earnings reports were downloaded through the use of these servers?
A. I did not come across that either.
Q. And this is despite a significant amount of effort being spent on your part to analyze these nine servers, correct?
A. I spent a lot of time examining these, yes.
Q. In fact, you produced a 136-page report outlining your
12:07 findings?
A. Yes.
Q. And one of the requests from Special Agent Hitchcock was to determine who was operating these servers; is that correct?
A. Yes.
Q. And were you able to ascertain who operated these servers?

A. I didn't identify who, but I found a lot of IP addresses, and I found information that -- some of the information we know about them, I guess.
Q. You have no knowledge whether Mr. Klyushin, for example, used any of the IP addresses that are associated with these servers, do you?
A. That was not my involvement. I provided Agent Hitchcock --
THE COURT: Can you answer that "yes" or "no"?
12:07 THE WITNESS: No.
BY MR. NEMTSEV:
Q. You testified to other programs, I believe, that were located on the server. One was PuTTY, correct?
A. Yes.
Q. Another one was NGINX, correct?
A. So PuTTY -- yeah, it was downloaded and NGINX, yes, was running on those machines, eight of the nine.
Q. And PowerShell Empire you testified to, correct?
A. Yes.
12:08 Q. And am I correct that all of that software is publicly available, open source, easily downloadable?
A. Yes.
Q. And its existence on a system does not necessarily indicate that it was a compromised or an infected computer, correct?

A. Well, I have log files that show that it was from infected machines and --
Q. You testified that a file was renamed, did you not?
A. Yes.
Q. You testified that, in your opinion, it was done in order to hide the program that was located within the file?
A. Yes.
Q. Is it your testimony that antivirus programs look at the name rather than the code of a program to determine whether it's malware or not?
A. I believe -- are you asking about PuTTY?
Q. I'm asking about the file that was renamed, I believe it was --
A. The migrate.exe?
Q. Potentially.
A. Yes. So migrate.exe, that was PuTTY, and PuTTY is not classified by Microsoft as malware. So Windows Defender is the default malware-scanning engine that's on most Windows operating systems, and it does not recognize PuTTY as malware.
Q. You would agree that a sophisticated actor, the way you phrase it, would know that Windows Defender doesn't identify this specific program, PuTTY, as malware?
A. They would know that. That was used to create a secure tunnel from the victim machine out to one of the hacker machines.

Q. And you would agree that if it's not identified as malware by Microsoft, for example, you wouldn't necessarily need to rename it in order to hide its origins or what it is?
A. Well, there may be system administrators that are looking at these log files, like the one on the right, and they -- if they see PuTTY running, for instance, that could raise suspicion. If they, for instance, aren't running Linux servers in their environment -- and I don't know all of the details of it, but -- of the victim environment, but if it's a Windows
12:10 environment and they see PuTTY running and they don't have any Linux or SSH servers, then that could potentially raise some concern from the sys admin.
Q. You also testified that you don't know what the Toppan Merrill administrators and what servers and what programs they were running, correct?
A. I don't know the details of their environment.
Q. You did not examine Toppan Merrill's service, correct?
A. I did not. I only examined the nine servers that I had.
Q. Sir, isn't it a fact that certain of the files that you
12:11 located and identified in your report originated from 2016?
A. Which ones are you referring to?
Q. Well, for example, 161 is an exhibit. It's a version of Mimikatz that was identified from 2016 -- November 26, 2016; is that correct?
A. Well, that may be when the developer wrote the code, not

necessarily when it was downloaded or set up or installed on the server number 8.

Q. Could you please take a look at page 60 of your report.

(Pause.)

A. Okay. I have it open here.

Q. Yes, of course. I don't expect you to memorize 136 pages of log files.

Am I correct that this is a printout of what you located on the C drive and program data?

12:12 A. This is one of the agent logs from server number 8.

Q. This is one of the agent logs?

A. So it's a log regarding one of the victim machines.

Q. So the data in C -- drive C program data that relates to data located on Toppan Merrill's server or the server of the hackers?

A. So this log file came from the hacker server, but it's about information in the victim computer.

Q. Can you turn to page 51, please.

A. Okay. I'm on page 51.

12:13 Q. Is my understanding correct that that is a file associated with the information of the computer that was potentially hacked belonging to Toppan Merrill?

A. Yes, it was identified on server number 8, and it is logged information from a victim machine.

Q. Do you see it says, "Original install date, August 4,

2016, 2:45 p.m."?
A. I'm looking for that line. One moment here.
Q. It's two or three --
THE COURT: Is it on the monitor?
MR. KOSTO: This isn't in evidence, your Honor.
MR. NEMTSEV: This is from his report, your Honor.
THE COURT: I see.
(Pause.)
A. Which location in the page is it?
12:14 Q. It's in the middle of the page, if you see -- if you have -- do you see where Merrill Corporation, registered owner?
A. Let's see. I see registered organization, Merrill Corp. Communications.
Q. Yes. And then two lines down, original install date?
A. Yes, I see that.
Q. And it refers to a date, August 4, 2016; is that correct?
A. Yes, this appears to be information about the Windows operating system install date, not the malware install date.
Q. At least the system itself was around since 2016, correct?
12:15 A. With the install date of Microsoft Windows, it appears to be, according to this log, August 4, 2016. So that was likely set up by probably an assist admin at the victim company, not the hackers.
Q. Understood.
A. They installed Windows.

MR. NEMTSEV: Nothing further, your Honor.
MR. KOSTO: Very briefly.
THE COURT: Why don't you ask from your -- well, if it's just a few questions.
MR. KOSTO: If that's okay, your Honor. From here?
THE COURT: Yeah, if it's just a couple of questions.

REDIRECT EXAMINATION

BY MR. KOSTO:

Q. You told Mr. Nemtsev that Mimikatz, PowerShell, and some of the other programs you referred to are able to be downloaded publicly; is that right?

A. Yes.

Q. Just because a program is -- like Mimikatz can be downloaded publicly, can it be used to steal passwords?

A. Yes.

Q. Is it allowable to use it to steal passwords?

MR. NEMTSEV: Objection.

THE COURT: Sustained.

BY MR. KOSTO:

Q. Do system administrators permit the use of Mimikatz to steal their passwords from their network?

MR. NEMTSEV: Objection.

THE COURT: Sustained.

A. I would say --

THE COURT: Sustained. You've got to listen to me.

I've agreed with the objection, so you can't answer.
BY MR. KOSTO:
Q. Mr. Uitto, are you familiar with the concept of exfiltration?
A. Yes.
Q. Big word, but what does it mean?
A. It means to steal data, take data.
Q. And in your review, did you find evidence -- you told Mr. Nemtsev you didn't find evidence of the taking of data from the
12:17 victim computers to these particular hacker servers; is that right?
A. That's right, but I did see secure tunnels that were created.
Q. So when you say there were secure tunnels, were you able to tell what was going through those secure tunnels?
A. No.
Q. Those were encrypted, right?
A. Yes.
Q. So you actually don't know whether or not there was
12:17 financial information in those tunnels?
A. That's correct.
Q. Or sports scores or anything?
A. That's correct.
Q. It's encrypted.
A. Yes.

Q. And why is it encrypted?
MR. NEMTSEV: Objection.
BY MR. KOSTO:
Q. What role does encryption serve in this hacker architecture?
MR. NEMTSEV: Objection.
THE COURT: Overruled.
A. So I can answer?
Q. Yes.
12:17 A. Yes, so it can be used to hide data or information.
Q. So if it's encrypted, we can't know what's being passed?
A. That's correct.
MR. KOSTO: Nothing further.
MR. NEMTSEV: A couple of questions.
Can I do it from here?
THE COURT: Right there.

RECROSS-EXAMINATION

BY MR. NEMTSEV:
Q. Isn't encryption a common security feature as well?
12:18 A. Yes, it's built into a lot of software these days.
Q. And system administrators obviously care about protecting their data, and they would use encryption, by themselves, to make sure that that data doesn't get out?
A. That's correct.
Q. And it's a common feature, we probably have it on our

phones, our computers, correct?
A. Yes, but I guess the usage that we see here with the migrate.exe, this was not run by the sys admin, it was run by a hacker.
THE COURT: I can't hear a word you're saying.
A. So the migrate.exe, the one that we looked at earlier, it was not run by a system administrator. It was run by one of the attackers.
Q. And what they took out or put in, you don't know, correct?
12:18 A. I don't know the contents.
MR. NEMTSEV: Thank you.
THE COURT: Thank you.
Thank you.
Who's the next witness?
You can step down. Thank you, sir.
MR. KOSTO: Vincent Kenney for -- the United States calls Vincent Kenney, your Honor.
May I take down the chalk?
THE COURT: Yes. And you'll get me a copy?
12:19 MR. KOSTO: Yes.
VINCENT KENNEY, having been duly sworn by the Clerk, was examined and testified as follows:
THE CLERK: You can be seated.
Could you please state and spell your last name for the record.

THE WITNESS: My last name is Kenney, and it's spelled K-e-n-n-e-y.

THE CLERK: Thank you.

DIRECT EXAMINATION

BY MR. KOSTO:

Q. Good afternoon, Mr. Kenney.

A. Good afternoon.

Q. Where do you work, sir?

A. I work for the Federal Bureau of Investigation for the Salt Lake City Division.

Q. Will you pull that mic nice and close?

A. I will. Is that good?

Q. What division?

A. The Salt Lake City Division.

Q. And what do you do for the FBI?

A. I'm a computer scientist.

Q. Is that something you studied in school?

A. It is.

Q. And do you have a Bachelor of Science degree?

A. I do.

Q. And when did you get that degree?

A. In 2013.

Q. Where did you first work out of college?

A. I worked for the Boeing Company as a software engineer.

Q. The airplane manufacturer?

THE COURT: You need to lean into that mic. Lean in, as they say.

THE WITNESS: Okay, get nice and close.

BY MR. KOSTO:

Q. You said Boeing. Is that the aircraft manufacturer?

A. It is.

Q. And how long did you work at Boeing?

A. For two-and-a-half years.

Q. After that what did you do?

12:20 A. I started my employment with the FBI.

Q. And so how long have you been at the FBI as a computer scientist?

A. Since October of 2015.

Q. Out there in Salt Lake, are you assigned to a particular squad that deals with virtual currency?

A. I am. I'm a member of the FBI's Virtual Currency Response Team.

Q. What is the Virtual Currency Response Team?

A. It's a collection of individuals in the FBI that are

12:21 subject matter experts in the area of virtual currencies.

Q. And as part of your work, do you analyze virtual currency transactions?

A. I do.

Q. And do you provide training on cryptocurrency or virtual currency to folks in the FBI?

A. I do.
Q. Do you provide trainings outside the FBI?
A. I do.
Q. Have you received any recognitions in relation to your work in virtual currency, digital currency?
A. I have.
Q. Specifically what?
A. I was recognized by the assistant director of the FBI's Criminal Investigation Division in 2020.
12:21 Q. For what, specifically?
A. For my work in the area of virtual currencies.
Q. How long have you been working in virtual currencies?
A. I've been working since 2015.
Q. And the Virtual Currency Response Team, when was that established?
A. That was established in early 2020.
Q. How many different investigations have you worked on related to virtual currencies?
A. Numerous different investigations.
12:22 Q. Can you describe the different types?
A. Yes. They've been computer intrusions, they've been just traditional white-collar crime cases, such as Ponzi schemes, and other different types of white-collar crime cases.
Q. Have you testified in criminal cases regarding cryptocurrency transactions?

A. I have.
Q. Have you testified as an expert in those cases?
A. I have.
MR. KOSTO: Your Honor, we'd offer Mr. Kenney pursuant to Rule 702.
THE COURT: He may offer an opinion.
BY MR. KOSTO:
Q. Let's start with a very basic question, Mr. Kenney.
In a sentence, what is virtual currency?
12:22 A. Virtual currency is simply a digital currency.
Q. And what is the most well-known digital currency?
A. Most well-known one is Bitcoin.
Q. And has your work in this case related to Bitcoin?
A. It has.
Q. Let's use Bitcoin as an example to explain some of this to us, okay?
Bitcoin's a digital currency, virtual currency?
A. It is.
Q. Can I use those terms to mean the same thing?
12:23 A. Generally interchangeable.
THE COURT: What does digital currency mean?
MR. KOSTO: That was my next question.
THE COURT: All right. I just need baby steps, walk us through this.
BY MR. KOSTO:

Q. What is digital currency, Mr. Kenney?
A. Yes. Digital currency is simply digital value that's used to buy or sell a service.
Q. So is it dollars?
A. It's not dollars; it's digital dollars, digital value.
Q. Is it associated with any particular country?
A. It is not.
Q. Is it backed by any particular government?
A. No, it's not.
12:23 Q. Why does digital currency -- or why does Bitcoin have value at all? Well, before I ask you that, what can you do with digital currency?
A. You can use digital currency to buy goods and services over the internet or other different places that accept that digital currency.
Q. So, for example, if I had Bitcoin and I wanted to rent a domain, could I use digital currency to do that?
A. You could use digital currency to purchase the renting and buying of that domain.
12:24 Q. Could I do it at a company like Namecheap?
A. You could.
Q. Are there banks that help people turn dollars into Bitcoin?
A. There are.
Q. And are there banks that help people turn Bitcoin into

dollars?
A. There are.
Q. Okay. So digital currency is just information, right?
A. Just digital value.
Q. Can I hold it in my hand?
A. No, you cannot.
Q. Where is it? Where is it stored?
A. It's stored on the internet, and it's stored on a ledger.
Q. What's the name of that ledger?
12:24 A. That is a blockchain.
Q. We'll come back to blockchain in a second.
But let's say I am wanting some Bitcoin, I want to rent a domain at Namecheap. Can you define two terms for us? The first of them is, are you familiar with the term "digital wallet"?
A. I am.
Q. And so I've got a wallet in my back pocket. How is a digital wallet different from this one?
A. A digital wallet is stored on a digital device such as a
12:25 cell phone or a computer or some other device that accepts wallet software.
Q. And so is it fair to say that a digital wallet is a place that you can store cryptocurrency?
A. It is.
Q. Or Bitcoin?

A. Or Bitcoin.
Q. So I need a digital wallet to be able to spend Bitcoin or receive Bitcoin?
A. To receive it, correct.
Q. There's one other term here. What about a Bitcoin address, what is that?
A. Yeah, so a Bitcoin address is a public address that stores the value of the cryptocurrency of the Bitcoin that you have.
Q. What's the real-world comparison to a Bitcoin address?
12:25 A. So it looks just like simple letters and numbers that are sort of put together.
Q. Is it like an account number for Bitcoin?
A. It's kind of like an account number, yes.
Q. So if I have an address, can I use that address to send and receive Bitcoin?
A. If you have an address, you can send Bitcoin from that address if there's value in it, and you can receive Bitcoin to that address.
Q. How many different addresses can I have?
12:26 A. You can have thousands of different addresses.
Q. And where would I keep all of my addresses to keep them organized?
A. You would keep that in a digital wallet.
Q. Okay. So my Bitcoin addresses where I keep the Bitcoin can go in a digital wallet?

A. Correct.
Q. And the digital wallet is software that helps me organize and spend my digital currency?
A. That's correct.
Q. Are we good so far?
A. We're good.
Q. Let's say I'm a person who now has a wallet and I have an address but I don't have any Bitcoin. What do I need to do to get it?
12:26 A. You would need to give your address to an individual that has cryptocurrency or has Bitcoin, and they would send value to that address.
Q. I don't have any Bitcoin, but if you gave me your address and I had an address, I could arrange to send it?
A. Yes. If you gave me your address and I had Bitcoin, I could send Bitcoin to your address.
Q. Okay. And how do you prove that you own the Bitcoin if you can't hold it in your hand and it's all going on up here in the air?
12:27 A. So the digital wallet contains your private key that's associated with that address.
Q. All right. So that's a new term.
What's a private key, and how does it relate to the Bitcoin in my address, in my wallet?
A. So a private key is used to prove you are the owner of

that address, of the Bitcoin address.
Q. Is it like a password for the wallet?
A. It's similar to a password, yes.
Q. And let's say I lose my password to my wallet and address.
A. If you can't recover that password and you lose it, then you lose access to that -- those funds in that address.
Q. But if I have the private key, if I have the password, what can I do with the Bitcoin in my wallet?
A. You can prove that you're the owner of the Bitcoin and
12:28 that address, and therefore, spend the funds from that address.
Q. And I believe you testified that you're familiar with the company Namecheap?
A. I am.
Q. What can one do at Namecheap?
A. An individual can purchase domain names at Namecheap.
Q. Can customers use Bitcoin from their own wallets to purchase domains at Namecheap?
A. They can use Bitcoin to purchase domains at Namecheap.
Q. One last concept to cover before we dig into your
12:28 analysis, Mr. Kenney.
You mentioned the blockchain. What is the blockchain?
A. The blockchain is a public record that stores all transactions that are made on the Bitcoin network.
Q. So if I sent you a Bitcoin, if I were so lucky as to have one, would it go to the blockchain -- or the record would go to

the blockchain?
A. The record of that transaction would go to the blockchain.
Q. And if you sent it on to Mr. Nemtsev, would that record go to the blockchain?
A. It would.
Q. And if Mr. MR. NEMTSEV sent it on to the Court, would that record go to the blockchain?
A. All records go to the blockchain.
Q. So it's kind of like a bank statement for all the Bitcoin
12:29 transactions?
A. That's publicly available.
Q. And so from the beginning of Bitcoin, all the way back, how many transactions are in the blockchain?
A. Millions of them.
Q. And maybe, I don't know, how many per month get generated on the Bitcoin blockchain?
A. Hundreds of thousands.
Q. And how many blockchains are there for Bitcoin?
A. There is one.
12:29 Q. Are there other virtual or digital currencies out there?
A. There are.
Q. Do they all have their own blockchains?
A. They do.
Q. And so what's the benefit of having this blockchain out there that you can look at?

A. It acts as a public record, so, therefore, people can confirm that -- an individual who owns cryptocurrency, they can confirm that information because it's publicly available.
Q. So if you have access to the blockchain, which we all do, what can you do when you've identified a particular virtual currency address in one of your cases?
A. You can look up to see where that address has been spent or received funds.
Q. So you're looking in the blockchain to see what you can
12:30 learn about that transaction?
A. Correct.
Q. Can I search the blockchain by name?
A. No, you cannot --
Q. Vincent Kenney, for example?
A. No, you cannot search it by a person's name.
Q. What can you search it by?
A. You can search it by the address or the transaction hash for that unique transaction.
Q. So that's a new term. So if I have your address, I can go
12:30 in and look for it in the blockchain?
A. Correct.
THE COURT: An IP address?
THE WITNESS: You won't need an IP address.
BY MR. KOSTO:
Q. When we say "address," we're referring to the Bitcoin

address?
A. That's correct.
THE COURT: The Bitcoin address, not the IP?
THE WITNESS: Correct.
BY MR. KOSTO:
Q. And that's a long series of letters and numbers?
A. Numbers and letters, yeah.
Q. How many letters and numbers go in each Bitcoin address? We're going to see a bunch.
12:31 A. Yeah, approximately 24.
Q. And that's the account number?
A. That's the public address, correct. That's the account.
Q. And so you can go into the blockchain and look for these addresses to try to trace the transactions?
A. Correct.
Q. Did you do some analysis regarding Bitcoin transactions in this case?
A. I did.
Q. And which transactions did you analyze?
12:31 A. I looked at three transactions that correspond to the purchasing of domains from Namecheap.
Q. And of the three transactions that you looked at, what is the first and last name of the customer associated with the first transaction?
A. So the first and last name is Andrea Neumann.

Q. And was there an email address for that person?
A. There was.
Q. What was it?
A. neumann@dr.com.
Q. I'm showing you Government's Exhibit 173B in evidence at page 1.
Do you recognize this document?
A. I do.
Q. And what is it?
12:32 A. This is the Namecheap record.
Q. And who is the first name, last name, and email for this particular account?
A. Andrea Neumann, and the email is neumann@dr.com.
Q. So this is one of the domain accounts that you were asked to analyze in this case; is that right?
A. Correct.
Q. Let me take you to page 4 of this Namecheap record.
In the bottom row of the page entitled "Transaction Review," could you share with us what we are looking at?
12:32 A. Yeah, you're looking at the purchasing record of information from Namecheap.
Q. So who bought what from Namecheap?
A. So Andrea Neumann purchased domains from Namecheap.
Q. And are you able to tell, looking at this record, how Andrea Neumann, or the Andrea Neumann subscriber, purchased

domains?
A. I am.
Q. How do you know?
A. I know because in the fourth column, the transaction type, I see that they were purchased through a service called BitPay.
Q. Okay. So we haven't heard BitPay before. What is BitPay, and how does that tell you that this is a purchase?
A. BitPay is a payment processor for cryptocurrencies.
Q. And what does BitPay -- what role does BitPay play in the digital currency environment?
A. So they act on behalf of their customer, Namecheap, to receive payment for the domain names or a good or service, and then they act kind of in the middle between Namecheap and the customer.
Q. So if I went to Namecheap to buy a domain, could I use a Mastercard?
A. You could.
Q. Could I use Visa?
A. You could.
Q. Could I use Bitcoin?
A. You could.
Q. Okay. And if I used Bitcoin to get something from Namecheap, what company would be involved?
A. It would go through BitPay.
Q. Let me point you, in Exhibit 173B, to the column that says

"CC Transaction ID."

Do you see it there?

A. I do.

Q. What is that transaction ID in the row related to BitPay?

A. That is the unique transaction ID that corresponds to the purchasing of cryptocurrencies through BitPay.

Q. Can I have you read the first four or five letters of that transaction ID?

A. It's 44L6.

12:34 Q. And the 44L6 transaction, what date did it take place?

A. It took place on August 15, 2018.

Q. And do you know whether the government obtained BitPay records related to the transaction that you've been describing on August 15, 2018?

A. I do.

Q. And where did the government get them?

A. They got them from BitPay.

Q. So do you recognize --

MR. KOSTO: Could we have Government Exhibit 181 in

12:35 evidence, please.

Q. Do you recognize Government's Exhibit 181?

A. I do.

Q. And what is it?

A. This is the records that came back from BitPay.

Q. And directing you to row 2 and Column A, can I have you

read the email address there?
A. That is neumann@dr.com.
Q. Is that the same email account we've been talking about for the last few minutes?
A. It is.
Q. And what is the date of the transaction in BitPay's records for the neumann@dr.com transaction?
A. August 15, 2018.
Q. And can I have you read the first few characters of the
12:35 string of letters and numbers in column H?
A. Yes, that is 44L6.
Q. And do you recognize that from anywhere?
A. I do.
Q. Where did that number come from?
A. That came from the previous record, the Namecheap record.
Q. So do we know that we're talking about the Namecheap transaction involving Andrea Neumann here?
A. That's correct.
Q. What is in column C of row 2 of Exhibit 181, the BitPay
12:36 record?
A. That is BitPay's public address.
Q. And can you just give us the first four letters of it?
A. 1JFS.
Q. Now, are BitPay addresses usually unique enough that you can read the first three or four letters and be pretty

confident that you're talking about the same wallet?
A. Yes.
Q. So we don't have to read all 26 letters every time?
A. No, we don't.
Q. So about this 1JFS record, whose address is that?
A. This is BitPay's address.
Q. And is this where BitPay receives its payment?
A. It is.
Q. Is this kind of similar to BitPay's cash register at the
12:36 front of the store?
A. Pretty much, yeah.
Q. So does BitPay receive a lot of payments, potentially,
into this one?
A. It could.
Q. Okay. And what did you do once you had an address that
was used to pay BitPay -- or you had the address that BitPay
got paid at. What was your next step in your analysis?
A. My next step was to see that on the blockchain.
Q. And why were you looking on the blockchain? What were you
12:37 trying to figure out?
A. I wanted to see who the sender of -- who the sender was
sending funds into this BitPay address.
Q. So who paid for Andrea Neumann's domain?
A. Correct.
Q. And can you tell the jury -- what's that process called?

A. That process is called blockchain analysis.
Q. Going to that public ledger?
A. Correct.
Q. Can you tell the jury in general terms how you start that analysis once you have an address that you want to know something about.
A. You'll take the address and you'll put it into a block explorer.
Q. What is a block explorer?
12:37 A. So a block explorer is an easier way to view these different transactions on a blockchain.
Q. A way of looking up on the blockchain to find information?
A. Correct.
Q. And in your experience, have you found the information in block explorer to be a reliable place to find information about Bitcoin transactions?
A. Yes, I have.
Q. And how do you know that it's accurate, using the block explorer instead of the blockchain itself?
12:38 A. Because I've actually downloaded the full Bitcoin blockchain and confirmed this information.
Q. God bless you.
Did you prepare an illustration in connection with your testimony today?
A. I did.

Q. And I'm showing you Government's Exhibit 189, just for the witness, if I can do that -- I can't do that.

THE CLERK: Can you hand it to him on paper?

THE COURT: Paper?

MR. KOSTO: This is Bitcoin testimony. We're not going to use paper.

May I approach the witness?

THE COURT: Yes.

(Discussion off the record.)

12:38 BY MR. KOSTO:

Q. Mr. Kenney, do you recognize Government's Exhibit 189?

A. I do.

Q. Would it assist you in explaining the Bitcoin tracing you conducted?

A. It would.

MR. KOSTO: I'd offer it and ask that it be published to the jury, at least page 1 of it.

THE COURT: I haven't seen it. Any objection?

MR. NEMTSEV: No objection, your Honor.

12:39 THE COURT: All right.

(Exhibit 189 received into evidence.)

BY MR. KOSTO:

Q. We're here at page 1, Mr. Kenney; is that right?

A. That's correct.

Q. And you've testified that you looked at a series of

Namecheap transactions in your analysis; is that right?
A. Correct.
Q. And are the three columns -- what are the three columns on page 1 of your illustration?
A. These are the three different accounts that are associated with these transactions.
Q. And so we -- let's look at Namecheap domain 1, that column. Can you read the buyer email?
A. The buyer email is neumann@dr.com.
12:39 Q. And can you read the transaction date?
A. Transaction date is August 15, 2018.
Q. And so this is the transaction that purchased from Namecheap on the Neumann account, correct?
A. Correct.
Q. And so can you share, in general terms, starting with that data point, what you were trying to show or determine with your analysis?
A. I was trying to show a relationship between these three different accounts.
12:40 Q. Can you go ahead and read the three accounts out loud, just from the starters? We'll get to each of them in turn, but you've read namecheap@dr.com. What's the next one?
A. The next one is kavin.sspender@mail.com.
Q. And what's the third account that you were trying to determine if there was a connection to?

A. The third account is wan-connie909@inbox.lv.
Q. And why did you look at these three accounts?
A. Because these were the three accounts that were given to me.
Q. If we could move to the next step of your process on page 2 of your illustration.
What was the first thing you did?
A. The first thing I did was I took that BitPay address that we saw in one of our earlier records --
12:40 Q. Is that the 1JFS?
A. That is.
Q. At the bottom right of your illustration?
A. Correct.
Q. Okay. And what did you do when you took that address?
A. I put that into a public block explorer.
Q. And why did you go to the block explorer with the 1JFS address?
A. Because I wanted to see the address that sent funds to it.
Q. And that's your starting point?
12:41 A. That is my starting point.
Q. And so let's go to page 3 of your illustration.
This is a little different. We've got -- is this from the block explorer?
A. This is from the blockchain.com block explorer, correct.
Q. We've got two blue boxes on this chart, right?

A. Mm-hmm.
Q. What is the blue box on the right?
A. The blue box on the right is the BitPay address, the familiar 1JFS address.
MR. KOSTO: Ms. Lewis, can you blow up the first few characters of the box on the right.
Q. So we have that there, the 1JFS.
A. Correct.
Q. That's the one you're trying to figure out who paid for it?
12:41
A. Correct.
Q. And you went to the block explorer to do that?
A. I did.
Q. And so that's the blue box on the right.
What's the blue box on the left?
A. The blue box on the left is the sender.
Q. This is the payer?
A. This is the person who paid.
Q. Can you read the first few characters of the payer's Bitcoin address?
12:42
A. It's 14KP.
Q. Okay. Do we have a date for this transaction from the blockchain explorer?
A. There is.
Q. And what is it?

A. It is August 15, 2018.
Q. Do you recognize that date?
A. I do.
Q. Is it the same date from the Namecheap records?
A. It is.
Q. So we know we're talking about the same transaction here?
A. Correct.
Q. Okay. And I want to direct you to the yellow highlighting in page 3 of your illustration.
12:42 Do you see it there?
A. I do.
MR. KOSTO: Could we have it a little bigger, please, Ms. Lewis. Thank you.
Q. Okay. We're looking at a long string here. Could you read the first five characters?
A. Yes. It's 1JMCC.
Q. And what is 1JMCC? That's a new address, we haven't seen that before.
A. It is.
12:43 Q. What is it?
A. It is the change from the sender for this transaction.
Q. What do you mean "the change"?
A. So when funds are sent from one Bitcoin address to another Bitcoin address, the remainder of the funds are put into a new address called the change address.

Q. So if I go to Target to buy something and I put my credit card down for a $15 item, or hand over $20 cash, I get change to me, right?
A. If you used a credit card, you wouldn't get any change. If you used cash, you might get some change.
Q. So why is Bitcoin -- if I sent $20 in Bitcoin, why am I getting change? Why can't I just send $15 in Bitcoin?
A. This is the nature of how the Bitcoin protocol works. It will move funds to this unspent address, and it's referred to as the change address.
Q. So if we can go back to page 3, if we have a total amount of Bitcoin, it all has to go, right?
A. It all goes into the change address.
Q. Some of it goes to pay for whatever you're buying, the rest of it goes to the change address?
A. Correct.
Q. And one more time, what is the change address that the change from the Andrea Neumann transaction went?
A. The change, exact change, is 0.0056.
Q. That's over there on the right?
A. Yes.
Q. That tells you how much change the address got?
A. Correct.
Q. And which address got the change?
A. The 1JMCC address.

Q. When you're tracing Bitcoin, what can you say about the wallet that paid for something and the wallet that got the change -- excuse me, the address that paid for something and the address that got the change?
A. So I can say that the address that paid for things, if it received the change, it's owned by the same owner.
Q. Even though it's a different address?
A. Even though it's a different address.
Q. Because the change goes to an entirely new address, right?
12:45 A. It goes to an entirely new address.
Q. But the sender of the money and the recipient of the change --
A. Are the same person.
Q. -- go together?
A. Correct.
THE COURT: How much longer do you think you have?
MR. KOSTO: We'll finish by 1:00, your Honor.
THE COURT: You'll finish yours by 1:00?
MR. KOSTO: Yes. Yes.
12:45 BY MR. KOSTO:
Q. So in this particular case, was there more payment or was there more change?
A. There was more change.
Q. And what date did the change transaction occur on?
A. Same date of August 15, 2018.

Q. That's the Neumann purchase date, right?
A. That's correct.
Q. So the change happens on the same day as the transaction?
A. Correct.
Q. So now you have a change address from the Neumann purchase, right?
A. Correct.
Q. What's the next step in your analysis?
A. My next step to see is where was the change spent.
12:45 Q. Let's look at Exhibit -- or page 4 of your illustration for a little recap here.
What is page 4 showing?
A. This is a recap of an earlier slide that simply shows me starting out with that familiar 1JFS BitPay address and tracing it backwards to see who was the sender.
Q. So that was the wallet number 1 here?
A. Correct.
Q. Okay. And let's add a little complexity here. Go to the next page of your illustration.
12:46 What have we added to the picture?
A. So in this illustration, we've added the fact that there is a change address for the remainder of the funds. That is address number 2.
Q. So how, in plain English, would you describe the contents of wallet number 2 at the left of your picture?

A. That is the remainder of the funds that the individual who owned wallet number 1 has been pushed into wallet number 2.
Q. And it's the change from what transaction?
A. It is the change from the transaction of Andrea Neumann for the BitPay purchase.
Q. At page 6 of the illustration, how did you continue your analysis?
A. I wanted to see where the funds from this change went to.
Q. And did you determine where the change -- where is the
12:47 change address in this page, number 6?
A. So the change address in this page is -- so the change address from the previous transaction in this one is 1JMCC.
Q. Where did 1JMCC send the change?
A. So it sent the funds to BitPay, the 1KwN address.
Q. So if BitPay received the change, were you able to determine what address or transaction BitPay got that change for?
A. Yes.
Q. And where did you find that?
12:47 A. I found that address listed here in the block explorer, but that was also one of the addresses that was given to me by the investigators.
Q. Let's go to Exhibit 182 in evidence.
Do you see the column C there?
A. I do.

Q. Can you read the first few letters of the address?
A. That is 1KwN.
Q. Is that the address that got the change from the Neumann transaction?
A. It is.
Q. And do Bitpay's records tell you what was purchased with the Bitcoin that went there?
A. They do.
Q. Well, for starters, for what company was the payment made?
12:48 A. The payment was made on behalf of Namecheap.
Q. It was another Namecheap transaction?
A. Correct.
Q. And what was the date of the Namecheap transaction?
A. That was October 29, 2018.
Q. And directing you to column P, what was the account associated with the Namecheap purchase?
A. That account is kavin.sspender@mail.com.
Q. So we have the change from Andrea Neumann making a purchase related to Kavin Spender's domain; is that right?
12:48 A. That's correct.
Q. Let's go to page 7 of your illustration.
And what's in the red box there?
A. That email address, kavin.sspender@mail.com.
Q. And which of the name -- which of the Namecheap transactions that you were asked to look at is Kavin Spender,

1, 2, or 3?
A. Number 2.
Q. So in plain English, at this point of your analysis, what has your analysis shown?
A. So I've shown that funds were used to purchase domains under account neumann@dr.com, and the change, the remainder of the funds, were then used to purchase accounts at kavin.sspender@mail.com.
Q. And how does that get at the question you're trying to answer?
A. So I'm trying to see if there's a relationship between these two accounts and these two Bitcoin payments.
Q. And what did you conclude so far?
A. So I concluded that the change, the remainder of funds, was used to spend and to purchase the second series of domains.
Q. And what does that tell you about the people or persons who did the second purchase?
A. That tells me there's a relationship between the two.
Q. Looking at page 8 of your illustration, where do we pick up now?
A. Now we pick up at the change address of this particular transaction.
Q. And when you say "this particular transaction," this is the change from what transaction?
A. The transaction under account kavin.sspender@mail.com for

domains under Namecheap.
Q. And on your illustration here at page 8, what is the change address, first few characters?
A. First few characters are 1DNG.
Q. And what was the date of the change transaction?
A. Same date, October 29, 2018.
Q. Same date as what?
A. Same date as the sending of the funds.
Q. So let's go to page 9 of your illustration for a bit of a recap.
12:50
There's a bit more here, but start with wallet 2 for us, up in the left-hand corner.
A. Wallet 2 is the change that came back from the initial purchase.
Q. Andrew Neumann?
A. Correct. Those funds then went to BitPay, and the change, so the remainder of those funds, went into another address listed as wallet number 3.
Q. So the diagonal line is the payment to Bitpay for the second account?
12:51
A. Correct.
Q. And the vertical line going down to wallet number 3 is the change, right?
A. It's the change.
Q. What was your next step?

A. Same pattern, follow the change to see where that was spend.
Q. Is that shown on page 10 of your illustration?
A. It is.
Q. And where did the change go from the purchase of the Kavin Spender domain?
A. So the change went into address 17zQ.
Q. And is that in the blue box on the right?
A. It is.
12:51 Q. When did that happen?
A. That happened on November 22, 2018.
Q. At what time? Does the blockchain explorer tell you what time the transaction was?
A. Yes, at 4:03:34 a.m.
Q. So at page 11 of your illustration, can we add this to the mix?
A. We can.
Q. And what do we have here in wallet 3?
A. We have the change from the kavin.sspender@mail.com going
12:51 into wallet number 3.
Q. Can we add page 12 of your illustration?
A. We can.
Q. What's new here?
A. So we see the funds that came from that change now go into a new recipient of 17zQ.

Q. And that's wallet 4?
A. And that's listed as wallet 4.
Q. So how does the money in wallet 4 relate to the Kavin Spender Namecheap transaction, that second transaction you testified about?
A. So the change from that Kavin Spender account went into wallet 4.
Q. And at page 13 of your illustration -- just a few more pages -- what did you do next?
12:52 A. I just wanted to see where those funds went to.
Q. The funds related to the Kavin Spender purchase?
A. Correct.
Q. And where did it go?
A. Those funds went into BitPay.
Q. And when did it go into BitPay?
A. Two hours later, at -- 11/22/2018 at 06:43.
MR. KOSTO: So if we can go back one slide -- two slides -- sorry, Ms. Lewis, three slides.
Q. The time that it arrived was what?
12:53 A. Approximately two hours later.
Q. So 4:34 a.m. it arrives?
A. It arrives in this new address at 4:35 -- or 4:34.
Q. And then when does it leave?
A. And then it leaves at approximately 6:43.
Q. And you mentioned that payment went where?

A. That payment went to BitPay.
Q. And were you able to determine if it was for a particular account?
A. I was.
Q. Let's go back to Exhibit 181 in evidence.
Do you recognize row 3, column C?
A. I do.
Q. What is that?
A. That is the public Bitpay address.
12:53 Q. That's the BitPay cash register?
A. Correct.
Q. And does the record at 182 show you what account was paid for using that address?
A. It does.
Q. And looking at column Q, what was -- well, what was the vendor related to this transaction?
A. The vendor was Namecheap.
Q. That's where we started with all this, right, back at Andrea Neumann?
12:53 A. That's correct.
Q. And we're back at Namecheap again?
A. We're back at Namecheap.
Q. And what was the account for this Namecheap purchase?
A. The account holder was wan-connie909@inbox.lv.
Q. Let me take to you forward to page 14 of your

illustration.

Do you recognize this from the beginning of your illustration?

A. I do.

Q. So where are we in your analysis now? You started us with a Namecheap purchase for Andrea Neumann. Where have we gotten?

A. We've gotten to the Namecheap domain number 3, so the far left column -- sorry, far right column.

Q. And how did we get from 1 to 3?

12:54 A. We got there because, one, we saw that account under neumann@dr.com, the funds were used to purchase that account, and then the change went to the next account, and that was used to purchase funds under kavin.sspender@mail.com. And then, shortly after, the recipient of funds used to purchase accounts under wan-connie909@inbox.lv.

Q. And what do you conclude from that data about those three accounts?

A. So I can conclude that there's a relationship between all three of these different accounts.

12:55 Q. Why would you say that?

A. Based off of the payment history and based off of the payment patterns.

Q. So what is page 15 of your illustration showing?

A. So this shows the conclusion of this pattern.

Q. Take us back to wallet 4.

What's been added since we last saw your illustration?
A. So wallet 4 is the recipient that received those change funds, and wallet 4 paid into BitPay.
Q. In relation to which account?
A. In relation to the wan-connie909@inbox.lv account.
Q. And you said something about the pattern being the reason for that conclusion. Why do you say "pattern"?
A. Because what we can see is that this followed the same pattern of the change moved from one account to another account
12:55 to another account. And the last hop that was made between 3 and 4, that address listed at number 4, that had never been used before. So that means that the owner of funds in number 3 had to have known the owner of funds in number 4 to receive that address and then send the funds across and finally purchase the last Bitpay account.
Q. Back at the beginning of our testimony, you told me that I'd need to know your address to be able to send you Bitcoin, right?
A. Correct.
12:56 Q. There's no place I can go up and look for your address?
A. If funds have never been sent to an address, it's not publicly on the blockchain. You have to receive it from someone.
Q. So the last page of your illustration, page 16. Do you see at the bottom there are two rows, "View IPs" and "Remote